DIPONEGORO LAW JOURNAL
Volume 11, Nomor 4, Tahun 2022
Website : https://ejournal3.undip.ac.id/index.php/dlr/

KEBIJAKAN PENAL PENANGULANGAN *CYBER TERRORISM* DI MASA SEKARANG MAUPUN DI MASA MENDATANG

Ilham Ghani*, Eko Soponyono, Mujiono Hafidh Prasetyo
Program Studi S1 Ilmu Hukum, Fakultas Hukum, Universitas Diponegoro
E-mail: ilhamghani29@gmail.com

Abstrak

Perkembangan teknologi informasi dan komunikasi tidak hanya memberikan dampak positif tetapi memberikan dampak negatif pula. Dampak negatif yang disebabkan oleh perkembangan tersebut adalah adanya bentuk kejahatan berupa siber terorisme yang merupakan bentuk dari kejahatan siber. Tujuan penelitian ini adalah mengungkap mengenai hukum positif di Indonesia guna menangani kejahatan siber teroris di masa sekarang dan bagaimana kebijakan hukum pidana di Indonesia pada masa mendatang. Penelitian ini menggunakan metode yuridis normatif. Hasil penelitian mengungkap bahwa hukum positif di Indonesia belum terdapat undang-undang yang secara eksplisit mengatur mengenai kejahatan siber terorirsme, baik dalam Kitab Undang-Undang Hukum Pidana, maupun dalam undang-undang terkait tindak pidana terorisme. Terdapat beberapa rumusan undang-undang di masa mendatang yang mengatur mengenai kejahatan siber yang di dalam-nya juga memuat kejahatan siber terorisme seperti yang ada dalam Rumusan Kitab Undang-Undang Hukum Pidana (RUU KUHP), oleh karenanya secepat perlu disahkan konsep RUU KUHP agar lebih optimal dalam menindak kejahatan siber terorisme.

Kata Kunci: KUHP; Tindak Pidana Siber; Terorisme.

Abstract

The development of information and communication technology not only has a positive impact but also has a negative impact. The negative impact caused by these developments is the existence of a form of crime in the form of cyber terrorism which is a form of cybercrime. Based on this background, this research was conducted with the aim of revealing the positive law in Indonesia to deal with cyber terrorist crimes in the present and how the criminal law policy in Indonesia will be in the future. This study uses a normative juridical method. The results of this study reveal that positive law in Indonesia does not yet have a law that explicitly regulates cyber-terrorism crimes, both in the Criminal Code, as well as in laws related to criminal acts of terrorism. There are several formulations of laws in the future that regulate cybercrimes which also contain cybercrimes of terrorism such as those in the Formulation of the Criminal Code (RUU KUHP), therefore it is necessary to ratify the draft Draft Criminal Code as soon as possible. to be more optimal in cracking down on cyber-terrorism crimes.

Keywords: *Penal Code; Cyber Crime; Terrorism.*

I. PENDAHULUAN

Teknologi informasi dan komunikasi merupakan hal yang tidak dapat dipisahkan dari kehidupan manusia untuk sekarang, karena pada masa kehidupan modern teknologi informasi sangat berguna mulai dari mencari informasi, menjalankan bisnis, politik, komunikasi. Hampir seluruh negara di dunia sangat bergantung pada teknologi informasi dan komunikasi. Teknologi informasi dan komunikasi bagai pedang bermata dua, yang disisi lain memberikan dampak positif bagi kehidupan manusia, namun pada sisi lain juga memberikan dampak negatif

pada kehidupan manusia. [1]Dampak negatif yang ditimbulkan oleh teknologi informasi adalah adanya suatu kejahatan *cybercrime*, yaitu kejahatan yang memanfaatkan komputer dan internet sebagai media untuk melakukan aksi kejahatan. Semakin pesatnya perkembangan teknologi informasi dan komunikasi juga dapat membawa bentuk-bentuk kejahatan konvensional menjadi bentuk kejahatan siber, diantaranya perang, kriminal maupun terorisme pada dasarnya merupakan bentuk kejahatan dengan menggunakan konsep tradisional, namun dengan perkembangan dunia internet sekarang terorisme berubah bentuk menjadi *cyberterrorism.* Pada dasarnya prinsip dibalik kejahatan terorisme fisik maupun *cyberterrorism* memiliki ancaman yang sama yaitu menimbulkan rasa takut kepada penduduk sipil. Berdasarkan kamus *Webster's New School and Office Dictionary* oleh noah webster, *A Fawcett Crest Book* disebutkan bahwa teror sebagai kata benda berarti *: Extreme afaer,* ketakutan yang amat sangat*. One who excite extreme afaer,* atau seseorang yang gelisah dalam ketakutan yang amat sangat. *The ability to cause such a faer*, kemampuan menimbulkan ketakutan.[2] Indonesia sendiri tidak termasuk dalam deretan teratas dalam daftar negara yang menjadi korban *cyber crime*, namun menjadi negara asal dimana *cyber crime* dilakukan. Lona Olavia melaporkan *"Indonesia has received greater scrutiny from cybercrime authorities in recent years, especially since a 2013 survey by Akamai Technologies, an IT security firm, reported that Indonesia had overtaken China as the number one source of hacking traffic in the world."* Indonesia telah mendapat pengawasan yang lebih besar dari pihak otoritas *cybercrime* beberapa tahun terakhir, terutama sejak survei tahun 2013 oleh Akamai Technologies, sebuah perusahaan keamanan TI, melaporkan bahwa Indonesia telah berhasil mengalahkan China sebagai sumber *hacking traffic* terbesar di dunia. Data tersebut tidak semata-mata diartikan bahwa pelaku berasal dari Indonesia, namun ada pelaku Warga Negara Asing yang melakukan kejahatan tersebut di Indonesia dengan menggunakan server Indonesia. Hal ini dilakukan karena pelaku melihat celah-celah hukum yang dapat diterobos oleh pelaku untuk terhindar dari jeratan hukum.[3]

Cyber Crime pada dasarnya merupakan suatu kejahatan yang melibatkan komputer dan jaringan (*net-work*). Penyalahgunaan komputer maupun jaringan dapat dilakukan oleh siapapun baik dilakukan dalam bentuk kelompok maupun individu dengan motif kriminal. Dalam pemahaman mengenai *cyber crime* terdapat beragam pandangan. *Cyber crime* sendiri memiliki dua asal kata, yakni '*cyber*' dan '*crime*'. Kata *'cyber'* merupakan singkatan dari *'cyberspace'*, yang berasal dari kata '*cybernetics'* dan 'space' isitilah *cyberspace* pertama kali uncul pada tahun 1984. William Gibson mendefinisikan *cyberspace* sebagai berikut:[4]

Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation . . ... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable

---

[1] Maskun. *Kejahatan Siber*. (Jakarta: Kencana Prenada Media Group,2012), hlm 15.
[2] Badan Pembinaan Hukum Nasional, NA Perubahan Undang-Undang Nomor 15 Tahun 2003

[3] Dewi Bunga, Politik Hukum Pidana Terhadap Penanggulangan *CyberCrime,*Jurnal UGM, hlm 3.
[4] Simon Nahak, Hukum Tindak Pidana Mayantara (*CyberCrime*) Dalam Prespektif Akademik, *Jurnal Prasada*, Vol. 4, No. 1, Maret 2017, 1-11, hlm 2.

complexity. Lines of light ranged in the nonspace of the mind, cluster and constellations of data. Like city lights, receding.

Menurut kepolisian Inggris *Cyber Crime* merupakan bentuk kejahatan yang menggunakan jaringan komputer untuk tujuan kriminal dan berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital[5].

The Prevention of Crime and The Treatment of Offlenderes di Havana, Cuba pada tahun 1999 dan di Wina, Austria pada tahun 2000, menyebutkan ada 2 istilah yang dikenal:

1. *Cyber crime* dalam arti sempit disebut computer crime, yaitu merupakan suatu perbuatan ilegal/melanggar yang secara langsung menyerang sistem keamanan komputer dan/atau data yang diproses oleh komputer.
2. *Cyber crime* dalam arti luas disebut *computer related crime*, yaitu perbuatan ilegal/melanggar yang berakitan dengan sistem komputer atau jaringan. Dari pengertian tersebut *cyber crime* dapat dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/alat komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan cara meruhikan pihak lain.

Penegakan hukum terkait *cyber terrorism* tidaklah mudah, mengingat karakteristik dari kejatahn tersebut. Beberapa yang menjadi kendala enanganan *cyber terrorism* antara lain:

a. Tidak ada definisi hukum yang secara pasti mengenai apa itu kejahatan *cyber terrorism* meskipun telah terdapat beberapa pendapat dari para ahli.
b. Formulasi hukum di Indonesia belum dapat menjangkau terkait perkembangan kejahatan pada dunia maya terutama pada *cyber terrorsim*, bahkan undang-undang yang terkait mengenai perlindungan data pribadi belum ada di Indonesia, dan untuk sementara ini pengaturan tentang kejahatan dunia maya didasarkan pada Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-undang Nomor 11 Tahun 2008.
c. Keunikan pada kejahatan dunia maya adalah kejahatan tersebut dapat melintasi sebuah yuridiksi negara, sementara itu masih sedikitnya perjanjian internasional yang mengatur mengenai penegakan hukum *cyber terrorism*.
d. Perlu adanya keseimbangan antara tindakan represif maupun preventif dalam mengatasi masalah *cyber terrorism*.
e. Kurangnya kewaspadaan para pengguna internet di tanah air yang memungkinkan menjadi suatu korban kejahatan siber, seperti memberikan identitas pribadi, foto, maupun video kepada orang yang baru saja dikenal.

Organisasi teroris memanfaatkan *Cyberspace* guna melancarkan serangan dari jarak yang sangat jauh meskipun target yang dituju berbeda negara bahkan benua sekalipun. Banyaknya sistem yang terkoneksi ke internet mempermudah mereka melakukan serangan terutama pada target yang berada dekat dengan mereka, penggunaan media internet juga meminimalisir jatuhnya korban dari pihak

[5] ITAC, IIIC Convention Views Paper On: Cyber Crime, IIIC 2000, Millenium Congress, Quebec, September 19th, hlm 2.

anggota teroris. [6] Istilah "kebijakan" berasal dari bahasa inggris "*policy"* (Inggris) dan "*politiek*" (Belanda). Pada dasarnya kebijakan merupakan sebuah pedoman maupun pelaksanaan dalam menetapkan sebuah peraturan yang lebih baik, serta dasar sebuah rencana dalam mewujudkan peraturan perundang-undangan di masa yang akan datang.

Pengertian politik hukum pidana menurut Soedarto dapat dilihat dari politik hukum maupun kriminal, menurut beliau "Politik Hukum" adalah:

1. Usaha untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi pada suatu saat.

Kebijakan dari negara melalui badan-badan yang berwenang untuk menetapkan peraturan-peraturan yang dikehendaki yang diperkirakan bisa digunakan untuk mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang dicita-citakan. Kebijakan atau politik hukum pidana juga merupakan bagian dari politik kriminal. Di lihat dari sudut politik kriminal, maka politik hukum pidana identik dengan pengertian kebijakan penanggulangan kejahatan dengan hukum pidana. Kebijakan atau upaya penanggulangan kejahatan pada hakikatnya merupakan bagian integral dari upaya perlindungan masyarakat (*Social Defence*) dan upaya mencapai kesejahterahan masyarakat (*Social Welfare*). Oleh karena itu, dapat dikatakan bahwa tujuan akhir atau tujuan utama dari politik kriminal adalah "perlindungan masyarakat untuk mencapai kesejahteraan masyarakat." Sedangkan "menurut Barda Nawawi Arief, dalam perspektif hukum pidana, upaya penanggulangan *cyber crime* dapat dilihat dari berbagai aspek, antara lain aspek kebijakan kriminalisasi (formulasi tindak pidana), aspek pertanggungjawaban pidana atau pemidanaan (termasuk aspek pembuktian dan alat bukti), dan aspek yurisdiksi.[7]

II. METODE PENELITIAN

Metode "penelitian yang digunakan adalah menggunakan metode yuridis normatif dengan studi literatur. Studi literatur meneliti data sekunder berupa bahan hukum primer dan bahan hukum sekunder. Dalam penelitian ini menganalisis Peraturan Perundang-Undangan yang berkaitan dengan tindak pidana penyebaran pornografi, yaitu KUHP, UU Tindak Pidana Terorisme dan UU ITE serta RUU KUHP yang di masa mendatang akan menjadi Peraturan Perundang- Undangan di Indonesia. Selain itu, dalam penelitian ini juga melakukan kajian perbandingan dengan negara- negara lain terkait dengan pengaturan tindak pidana cyber terorism." Metode "yang digunakan untuk menganalisis data yang terkumpul dalam penelitian ini adalah metode analisis kualitatif. Penelitian yuridis normatif yang bersifat kualitatif adalah penelitian yang mengacu pada norma hukum yang terdapat dalam peraturan perundang-undangan dan putusan pengadilan serta norma-norma yang hidup dan berkembang dalam masyarakat.

---

[6] Brenner, Susan W. *Cybercrime: Criminal Threats from Cyberpsace*. (New Delhi:Pentagon Press, 2008), hlm 153.

[7]Barda Nawawi. Bunga Rampai Kebijakan Hukum Pidana. (Jakarta: PT Fajar Interpratama Mandiri, 2014), hlm 14.

III. HASIL DAN PEMBAHASAN

A. Bagaimana kebijakan penal dalam pencegahan cyberterrorism di masa sekarang

Kemajuan teknologi yang tidak sertamerta hanya membawa dampak positif bagi kehidupan umat maunusia juga membawa dampak lain, dengan kata lain kemajuan teknologi berimplikasi pada kejahatan. Perubahan yang terjadi akibat adanya perkembangan tersebut berdampak pada kejahatan tradisional yang kini bertransformasi menjadi suatu kejahatan dunia maya (*Cybercrime*) dengan memanfaatkan media elektronik serta internet sebagai alat. Penggunaan internet dapat diakses siapapun tanpa memandang umur maupun gender, dengan adanya kemudahan dalam mengakses internet, masyarakat dapat menjadi sebuah sasaran dari kejahatan tersebut tanpa kecuali.

Penegakan hukum terkait *cyber terrorism* tidaklah mudah, mengingat karakteristik dari kejatahn tersebut. Beberapa yang menjadi kendala penanganan *cyber terrorism* antara lain:

a. Tidak ada definisi hukum yang secara pasti mengenai apa itu kejahatan *cyber terrorism* meskipun telah terdapat beberapa pendapat dari para ahli.
b. Formulasi hukum di Indonesia belum dapat menjangkau terkait perkembangan kejahatan pada dunia maya terutama pada *cyber terrorsim*, bahkan undang-undang yang terkait mengenai perlindungan data pribadi belum ada di Indonesia, dan untuk sementara ini pengaturan tentang kejahatan dunia maya didasarkan pada Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-undang Nomor 11 Tahun 2008.
c. Keunikan pada kejahatan dunia maya adalah kejahatan tersebut dapat melintasi sebuah yuridiksi negara, sementara itu masih sedikitnya perjanjian internasional yang mengatur mengenai penegakan hukum *cyber terrorism*.
d. Perlu adanya keseimbangan antara tindakan represif maupun preventif dalam mengatasi masalah *cyber terrorism*.
e. Kurangnya kewaspadaan para pengguna internet di tanah air yang memungkinkan menjadi suatu korban kejahatan siber, seperti memberikan identitas pribadi, foto, maupun video kepada orang yang baru saja dikenal.

Politik kriminal (*criminal policy*) adalah usaha rasional untuk menanggulangi kejahatan. Dalam politik hukum pidana terdapat sebuah pedoman dalam menetapkan kebijakan penal maupun non penal. Melaksanakan politik hukum pidana merupakan hal penting dalam bidang pidana, dengan menerapkan politik hukum pidana berarti terdapat usaha untuk memformulasikan perundang-undangan sesuai dengan situasi maupun kondisi di masa yang akan datang. Dalam pembentukannya, undang-undang terbentuk karena adanya proses sosial serta proses politik yang memiliki peranan penting guna mengatur maupun mengendalikan masyarakat. Selain hal tersebut melakukan kriminalisasi merupakan kebijakan dalam menetapkan suatu perbuatan yang tidak dapat dipidana menjadi perbuatan yang dapat dipidana untuk menjangkau tindakan *cyber terrorism* dengan mempertimbangkan berbagai aspek dari perumusan delik,

pertanggungjawaban pidana hingga sanksi pidana yang dapat diterapkan bagi tindak pidana *cyber terrorism*.

Kebijakan penal pada masa sekarang yang dapat dikaitkan dengan adanya tindak pidana *cyber terrorism* dapat di uraikan sebagai berikut:

1. Kitab Undang-Undang Hukum Pidana

Berdasarkan apa yang telah dimuat dalam KUHP sekarang ini masih banyak delik yang bersifat konvensional serta belum terjangkaunnya jenis tindak pidana yang berkaitan dengan *cyber crime* terutama pada masalah *cyber terrorism*. Masih banyaknya tindak pidana konvensional yang diatur dalam KUHP, maka KUHP memiliki keterbatas dalam menanggulangi tindak pidana yang bersifat *high-tech* dengan macam variannya. Salah satu keterbatasan yang dimiliki KUHP sendiri ialah masalah pemidanaan pada seorang yang melakukan aktivitas hacking, yang dimana hacker secara illegal menerobos masuk guna mendapatkan akses tidak sah ke komputer, jaringan, sistem komputasi, perangkat seluler, atau sistem. Apabila pada kasus tersebut dikenakan pasal yang terdapat pada KUHP pasal yang mendekati ialah pasal 167 (1) KUHP padahal yang dimasudkan hacking adalah berusaha mendapatkan akses penuh terhadap sebuah komputer secara illegal dan apabila dikenakan pasal 167 KUHP maka akan adanya analogi hukum, yang seharusnya analogi pada pasal KUHP tidak diperkenakan dikarenakan akan melanggar ketentuan dari pasal 1 KUHP mengenai asas legalitas. Keterbatasan-keterbatasan tersebut lah yang menyebabkan tidak dapat dijangkaunya kejahatan *high-tech crime*.

Apabila KUHP akan digunakan pada pelaku kasus *cyber terrorism* hendaklah memperhatikan unsur maupun ruang lingkup dari *cyber terrorism*. Secara singkat penulis merumuskan unsur-unsur *cyberterrorism* diantaranya:

a. Serangan maupun ancaman terhadap komputer, jaringan dan informasi yang ditujukan kepada pemerintah maupun rakyat untuk kepentingan politik dan sosial dari para terorirsme.
b. Selanjutnya, untuk memenuhi syarat sebagai terorisme siber,suatu serangan harus mengakibatkan kekerasan terhadap orang atau harta benda, atau setidaknya menyebabkan timbulnya rasa takut. Serangan yang menyebabkan kematian atau cedera tubuh, ledakan, atau kerugian ekonomi yang parah.
c. Serangan *cyber terrorism* dapat dilakukan dari jarak yang sangat jauh baik dari serangan negara ke negara maupun ke antar benua. (tidak bergantung pada jarak).
d. Serangan yang ditumbulkan dapat mengakibatkan pemusnahan masal, apabila serangan ditujukan kepada infrastruktur yang terkoneksi pada jaringan internet.

2. Peraturan di luar Kitab Undang-Undang Hukum Pidana

Terdapat beberapa undang-undang di luar KUHP yang mengatur mengenai kejahatan yang memanfaatkan kecanggihan teknologi informasi dan elekronik diantaranya adalah:

a. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 11 Tahun 2008 merupakan undang-undang pertama di Indonesia yang secara khusus mengatur mengenai kejahatan siber. Pembentukan

undang-undang ini merupakan wujud dari harmonisasi terkait instrumen-instrumen internasional mengenai *computer related crime* seperti yang telah disebut pada beberapa instrumen seperti *Eu Convention article 11*

1. *Each Party shall adopt such legislative and other measures as maybe necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.*
2. *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention.*

b. Undang-Undang Nomor 5 Tahun 2018 *juncto* Perppu Nomor 1 Tahun 2002 tentang Tindak Pidana Terorisme

Terjadinya peledakan bom Bali telah mem-bawa beberapa dampak penting bagi kebija-kan politik keamanan Indonesia. Pertama, pemerintah segera menerbitkan Peraturan Pemerintah Pengganti Undang-undang (Perppu) Nomor 1 Tahun 2002 tentang Pemberantasan Terorisme, serta Perppu Nomor. 2 Tahun 2002 tentang penggunaan Perppu Nomor 1 untuk melakukan penyidikan terhadap kasus peledakan bom di Kuta Bali. Kedua, peme-rintah menyatakan organisasi Jamaah Islamiyah sebagai organisasi teroris yang ber-tanggungjawab atas terjadinya aksi peledakan bom di Bali dan lewat Departemen Luar Negeri mendaftarkan organisasi Jama'ah Islamiyah sebagai organisai teroris yang selu-ruh kegiatannya dapat dikategori-kan melang-gar Perppu Nomor 1 Tahun 2002.[8]

Selain itu, adanya komitmen masyarakat Internasional dan mencegah dan memberantas terorisme sudah diwujudkan dan berbagai konvensi Internasional yang menegaskan bahwa terorisme merupakan kejahatan yang bersifat internasional yang mengancam perdamaian dan kedamaian umat manusia sehingga seluruh anggota perserikatan Bangsa-Bangsa (PBB) termasuk Indonesia wajib mendukung dan melaksanakan revolusi Dewan Keamanan PBB yang mengutuk dan menyerukan seluruh anggota PBB untuk mencegah dan memberantas terorisme melalui pembentukan peraturan undang-undang nasional negaranya. Pemerintah Republik Indonesia telah merespon upaya dan kiat untuk mengantisipasi dan mengatasi tindakan terorisme itu dengan sekaligus disahkannya dua Undang-Undang, yaitu Undang-Undang RI Nomor 16 Tahun 2003 tentang penetapan peraturan pemerintah pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Terorisme.

Studi Perbandingan

Mengingat *cyberspace* memiliki perubahan yang kian pesat dan memiliki sifat global mengakibatkan bentuk *cybercrime* dimasa yang akan datang sangat sulit diprediksi, yang nantinya juga akan menyulitkan para legislator dalam proses kriminalisasi. Sehubung dengan adanya hal tersebut Komisi Presiden AS pada

[8] https://ylbhi.or.id/publikasi/terorisme-dan-perppu-no-1-tahun-2002/ (Diakses pada 21 Mei 2022)

tahun 1986 pernah mengutarakan pernyataan sebagai berikut: "Kejahatan bukanlah merupakan fenomena tunggal yang sederhana yang dapat diteliti, dianalisa, dan diuraikan dengan secara ringkas. Kejahatan terjadi di setiap sudut negeri dan terdapat pada setiap lapisan masyarakat. Pelaku kejahatan dan korbannya meliputi semua umur, penghasilan dari berbagai latar belakang hidup masing-masing"

Perkembangan teknologi yang pesat mendorong Indonesia untuk membentuk aturan guna mencegah maupun menindak para pelaku kejahatan, mengingat sifat *cybercrime* yang *borderless* dalam upaya kriminalisasi harus memperhatikan perkembangan upaya penanggulangan baik hukum regional maupun internasional dalam rangka harmonisasi hukum. Salah satu instrumen hukum internasional *eu convention articles 23* menyebutkan bahwa:

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Adanya pernyataan seperti instrumen hukum tersebut, metode perbandingan hukum merupakan suatu upaya yang dapat diterapkan guna membentuk sebuah aturan yang lebih ideal. Soerjono Soekanto beperndapat bahwa perbandingan hukum mungkin diterapkan dengan memakai unsur-unsur sistem hukum sebagai titik-tolak perbandingan. Sistem hukum mencakup tiga unsur pokok, ialah:

a. Struktur hukum yang mencakup lembaga-lembaga hukum,
b. Substansi hukum yang mencakup perangkat kaidah atau perilaku teratur, dan
c. 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.[9]

Cyber terrorism yang pada dasarnya merupakan salah satu bentuk *cyber crime* merupak jenis kejahatan yang perlu diwaspadai karena mereka berbentuk *high-tech crime* dimana pengaturan mengenai kejahatan *high-tech crime* di Indonesia belum berjlan seperti yang seharusnya. Dengan adanya metode perbandingan hukum diharapkan Indonesia dapat membentuk peraturan guna mencegah terjadinya aksi *cyber crime* baik melalui kebijakan preventif maupun represif. Ancaman *cyber terrorism* yang tidak dapat disepelekan juga pernah diungkapkan oleh penasihat keamanan gedung putih pada konferensi keamanan RSA di San Francisco, CA 25 Februari 2004. menyatakan bahwa potensi serangan *cyber teroris* adalah nyata.

Dalam makalah mereka, Jimmy Sproles dan Will Byars mengatakan:

By the use of the internet the terrorist can affect much wider damage or change to a country than one could by killing some people. From disabling a

[9] Barda Nawawi Arief, *Perbandingan Hukum Pidana*. (Jakarta: Rajawali Pers,2014), hlm 12.

countries military defenses to shutting off the power in a large area, the terrorist can affect more people at less risk, than through other means

Pernyataan jim dan will kemudian disusul oleh pendapat dari *Senator Jon Kyl, chairman of the senate judiciary subcommittee on terrorism, technology and homeland security mentioned that members of al-Qaeda have tried to target the electric power grids, transportation systems, and financial institutions.In England the National High-Tech Crime Unit (NHTCU) survey showed that 97% of the UK companies were victims to cyber crime during the period from June 2002 to June 2003.Cyber terrorists can endanger the security of the nation by targeting the sensitive and secret information (by stealing, disclosing, or destroying).*[10]

Pembentukan undang-undang yang mengatur secara khusus tentang *cyber crime* merupakan hal yang sangat penting terlebih kejahatan tersebut merupakan *extra ordinary crime* yang dimana memerlukan penanganan khusus. Dalam bukunya Widodo mengutarakan terdapat 4 alternatif guna menangani *cyber crime* yaitu:

1. Memperluas pengertian maupun istilah tertentu melalui penafsiran hukum pada KUHP konvensional.
2. Melakukan amandemen KUHP.
3. Menerbitkan peraturan secara khusus yang mengatur *cyber crime* yang didalamnya juga terdapat delik mengenai *cyber terrorism.*
4. Mengamandemen KUHP sekaligus menerbitkan Undang-Undang khusus yang mengatur *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.

SINGAPURA

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

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

[10] Mudawi Mukhtar Elmusharaf (2004) Cyber Terrorism : The New Kind of Terrorism

2) *"This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years."*
3) *"Any person guilty of an offence under this section shall be liable on conviction to a not exceeding $50.000 or to imprisonment for a term not exceeding 10 years pr to both."*

AMERIKA

Di Amerika terdapat suatu peraturan khusus terkait tindak pidana *cyber* yang mengarah pada perbuatan *cyber terrorism* pada *Accessing a Computer and Obtaining Information: 18 U.S.C. 1030(a)(3) Title 18, United States Code, Section 1030(a)(3) provides: Whoever— (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct afects that use by or for the Government of the United States . . . shall be punished as provided in subsection (c) of this section.*

"Nonpublik" mencakup sebagian besar komputer pemerintah, tetapi bukan server Internet yang, menurut desain, menawarkan layanan kepada anggota masyarakat umum. Misalnya, server database lembaga pemerintah mungkin "nonpublik", sedangkan server web lembaga yang sama adalah "publik".

Komputer harus dimiliki atau dikendalikan oleh departemen atau agen Amerika Serikat, atau setidaknya digunakan "oleh atau untuk" pemerintah Amerika Serikat dalam kapasitas tertentu. Misalnya, jika Amerika Serikat telah memperoleh akun di server perusahaan swasta, server tersebut digunakan "oleh" Amerika Serikat meskipun tidak dimiliki oleh Amerika Serikat. Pelanggaran bagian ini dapat dihukum dengan denda dan hingga satu tahun penjara, 18 USC 1030(c)(2)(A), kecuali individu tersebut sebelumnya telah dihukum atas pelanggaran bagian 1030, dalam hal ini hukuman maksimum meningkat menjadi sepuluh tahun penjara, 18 USC 1030(c)(2)(c). *except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph.*

B. Bagaimana kebijakan penal dalam pencegahan cyberterrorism di masa mendatang

Meningkatnya penggunaan internet dapat memberikan dampak positif bagi beberapa orang, disaat yang sama pula dapat memberikan kemudahan bagi pengguna internet dalam hal melalukan suatu tindak pidana.

Munculnya beragam jenis kejahatan *cyber* termasuk *cyber terrorism* dapat disebabkan oleh beberapa faktor keamanan, selain itu kurangnya wawasan para penegak hukum dalam menindak para pelaku kejahatan *cyber*, serta belum adanya undang-undang yang mengatur secara khusus mengenai *cyber crime* dan dapat memberikan celah bagi para pelaku tindak pidana *cyber terrorism*.

Kongres PBB VIII/1990 mengenai *"Computer-related crimes"* dalam upaya menanggulangi kejahatan *cyber terrorsim* mengajukan beberapa kebijakan antara lain:

1. Menghimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:

a. Melakukan modernisasi hukum pidana
b. Mengembangkan tindakan-tindakan pencegahan keamanan komputer
c. Melakukan sosialisasi hukum kepada masyarakat mengenai *cyber terrorsim* serta memberikan wawasan bagi para penegak hukum terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer.
d. Melakukan training bagi para hakim, pejabat dan aparat penegak hukum mengenai *cyber crime*.

2. Menghimbau negara anggota meningkatkan kegiatan nasional dalam upaya penangggulangan *cyber terrrosim* yang juga sebagai bentuk kejahatan *cyber*.

Berkaitan dengan resolusi kongres PBB VIII/1990 terkait *computer-related crime*, bahwa dalam upaya penanggulangan *cyber terrorism* Indonesia dituntut untuk melakukan modernisasi hukum pidana. Dalam seminarnya Wigrantoro Roes Setiyadi mengenai *Cyber crime* tanggal 19 Maret 2003 beliau menawarkan alternatif diantaranya adalah:

1. Menghapus pasal-pasal dalam UU terkait yang tidak dipakai lagi.
2. Mengamandemen KUHP.
3. Mensisipkan hasil kajian dalam RUU yang ada.
4. Membuat RUU khusus *cyber crime*.[11]

Apabila dibandingkan dengan beberapa negara tetangga Indonesia merupakan salah satu negara yang tidak memiliki undang-undang khusus *cyber crime* dan belum melakukan amandemen terhadap KUHP yang pasal-pasalnya masih mengatur kejahatan konvensional dan tidak relevan dengan *cyber terrorism* yang menggunakan media komputer dan internet sebagai sarana tindak pidana. Namun untuk saat ini Indonesia sudah berupaya dalam pembuatan RUU yang mengatur *cyber crime* diantaranya ialah:

1. RUU tentang Kitab Undang-Undang tahun 2019
2. RUU tentang Pemanfaatan Teknologi Informasi (PTI)
3. RUU tentang Tindak Tidana di Bidang Teknologi Informasi (TPTI)
4. RUU tentang Informasi, Komunikasi, dan Transaksi Elektronik (IKTE)

Ketentuan-ketentuan pada rancang tersebut dapat uraikan sebagai berikut:

RUU TPTI berkaitan dengan *Cyber Crime*

Pasal 8

Setiap orang yang dengan sengaja dan melawan hukum memanfaatkan teknologi informasi dengan maksud untuk menghilangkan nyawa, harta benda orang lain, atau mengakibatkan kerusakan atau kehancuran obyek-obyek vital dan strategis atau lingkungan hidup atau fasilitas umum atau fasilitas internasional usaha menggulingkan pemerintahan yang sah, atau membahayakana kemaanan

[11] Abdul Wahid, Mohammad Labib, *Kejahatan Mayantara* (Bandung:Refika Aditama, 2005), hlm 73.

negara atau untuk memisahkan sebagian dari wilayah negara atau sebagai bagian dari kegiatan teror kepada orang atau negara lain, dipidanan dengan pidana mati atau penjara seumur hidup atau pidana penajra, paling singkat 10 (sepuluh) tahun dan paling lama 20 (dua puluh) tahun.

Pasal 10

Setiap orang yang dengan sengaja dan melawan hukum memasuki lingkungan dan atau saran fisik Sistem Informasi tanpa hak atau secara tidak sah menggunakan sandi akses palsu, melalukan pembongkaran tanpa seijin pemiliknya yang sah atau perusakan dengan atau tanpa maksud merugikan pemilik sah, dipidana paling singkat 2 (dua) tahun dan paling lama 4 (empat) tahun atau denda sedikit-dikitnya Rp200.000.000,00 (dua ratus juta rupiah). Dan sebanyak-banyaknya Rp800.000.000,00 (delapan ratus juta rupiah).

Pasal 11

(1) Setiap orang yang dengan sengaja dan melawan hukum memasuki lingkungan dan atau sara fisik Sistem Informasi milik instansi pemerintah, meliter, perbankan, atau instansi strategis lainnya tanpa hak atau secara tidak sah dengan menggunakan sandi akses palsu, melakukan pembongkaran atau perusakan dengan atau tanpa amksud merugikan instansi yang ditujum dipidana penjara paling singkat 7 (tujuh) tahun dan paling lama 12 (dua belas) tahun atau denda sedikit-dikitnya Rp700.000.000,00 (tujuh ratus juta rupiah) dan sebanyak-banyaknya Rp 1.500.000.000,00 (satu miliyar lima ratus juta rupiah).
(2) Apabila pelaku kejahatan dimaksud ayat (1) terbukti telah menyebarkan dan atau mengumumkan informasi yang harus dilindungi kepada pihak yang tidak berwenang, dipidana penjara sesuai ayat (1), ditambah (2) tahun.

Pasal 13

Setiap orang yang dengan sengaja dan melawan hukum, memasukan, mengubah, menghapus atau menghilangkan sebagian data komputer atau menggangu sistem komputer, yang menimbulkan kerugian bagi orang lain, dipidana penjara paling singkat 3(tiga) tahun dan paling lama 7 (tujuh) tahun, dan dikenakan denda sedikit-dikitnya 3(tiga) kali dari nilai kerugian yang ditimbulkan.

RUU KUHP 2019

Paragraf 1, Penggunaan dan Perusakan Informasi Elektronik

Pasal 336

Setiap Orang yang menggunakan atau mengakses Komputer atau sistem elektronik dengan cara apapun tanpa hak dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam Komputer atau sistem elektronik dipidana dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori V.

Paragraf 2 Tanpa Hak Mengakses Komputer dan Sistem Elektronik

Pasal 337

Dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak kategori VI.

Pasal 339

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

IV. SIMPULAN

Berdasarkan hasil pembasan di atas bahwasanya di Indonesia belum terdapat peraturan yang secara eksplisit mengatur tindak pidana *cyber terrorism* baik dalam UU ITE maupun undang-undang terorisme, oleh karenanya masih dalam hal menindak para pelaku kejahatan siber masih belum maksimal dan masih terdapat penggunaan-penggunaan pasal yang tidak semestinya seperti penerapan pasal dalam KUHP yang dikenakan pada pelaku tindak kejahatan siber.

Berdasarkan hasil penelitian di atas, kebijakan penal penanggulangan di masa mendatang telah di rumuskan dalam beberapa rancangan undang-undang terkait *cyber crime* dan telah diatur juga pada RUU KUHP. Oleh karenanya pengesahan RUU KUHP sangatlah penting karena dalam pembentukan rancang undang-undang terkait *cyber terrorism* diperlukan RUU KUHP sebagai payung hukum daripada *cyber law.*

DAFTAR PUSTAKA

Abdul Wahid, Mohammad Labib, Kejahatan Mayantara (Bandung:Refika Aditama, 2005)

Badan Pembinaan Hukum Nasional, NA Perubahan UU Nomor 15 Tahun 2003

Barda Nawawi. Bunga Rampai Kebijakan Hukum Pidana. (Jakarta: PT Fajar Interpratama Mandiri, 2014)

Barda Nawawi Arief, Perbandingan Hukum Pidana. (Jakarta: Rajawali Pers,2014)

Brenner, Susan W. Cybercrime: Criminal Threats from Cyberpsace. New Delhi:Pentagon Press, 2008)

Dewi Bunga, Politik Hukum Pidana Terhadap Penanggulangan CyberCrime, Jurnal UGM

ITAC, IIIC Convention Views Paper On: Cyber Crime, IIIC 2000, Millenium Congress, Quebec, September 19th,

Kitab Undang-Undang Hukum Pidana

Maskun. *Kejahatan Siber*. (Jakarta: Kencana Prenada Media Group,2012)

Mudawi Mukhtar Elmusharaf (2004) Cyber Terrorism : The New Kind of Terrorism

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

Simon Nahak*, Hukum Tindak Pidana Mayantara (CyberCrime) Dalam Prespektif Akademik,* Jurnal Persada

Terorisme dan Perppu No.1 Tahun 2002, https://ylbhi.or.id/publikasi/terorisme-dan-perppu-no-1-tahun-2002/

Undang-Undang Informatika dan Transaksi Elektronik

Undang-Undang Nomor 15 tahun 2003