TINJAUAN YURIDIS TINDAK PIDANA *CYBER TERRORISM* DALAM PERSPEKTIF KEJAHATAN TRANSNASIONAL TERORGANISIR

SKRIPSI

Disusun untuk memperoleh gelar Sarjana Hukum

Oleh

OKTI PUTRI ANDINI

8111416215

PROGRAM STUDI ILMU HUKUM

FAKULTAS HUKUM

UNIVERSITAS NEGERI SEMARANG

2020

PERSETUJUAN PEMBIMBING

Skripsi dengan judul "Tinjauan Yuridis Tindak Pidana *Cyber terrorism* dalam Perspektif Kejahatan Transnasional Terorganisir", disusun oleh Okti Putri Andini (8111416215) telah disetujui untuk dipertahankan di hadapan Sidang Ujian Skripsi Fakultas Hukum Universitas Negeri Semarang, pada:

Hari : Senin

Tanggal : 16 Maret 2020

Pembimbing,

Sonny Saptoajie Wicaksono, S.H., M.Hum

NIP. 197610232008121006

Mengetahui,

Wakil Dekan Bidang Akademik

Fakultas Hukum UNNES

Prof. Dr. Martitah, M.Hum.

NIP. 196205171986012001

PENGESAHAN

Skripsi dengan judul **"Tinjauan Yuridis Tindak Pidana *Cyber terrorism* dalam Perspektif Kejahatan Transnasional Terorganisir"**, disusun oleh Okti Putri Andini (8111416215), telah dipertahankan di hadapan Sidang Ujian Skripsi Fakultas Hukum Universitas Negeri Semarang, pada:

Hari : Selasa

Tanggal : 14 April 2020

Menyetujui,

Penguji Utama,

Dr. Ali Masyhar, S.H., M.H.

NIP. 197511182003121002

Penguji I

Anis Widyawati, S.H., M.H.

NIP. 197906022008012021

Penguji II

Sonny Saptoajie Wicaksono, S.H., M.Hum.

NIP. 197610232008121006

Mengetahui,

Dekan Fakultas Hukum UNNES

Dr. Rodiyah, S.Pd., S.H., M.Si.

NIP. 197206192000032001

HALAMAN PERNYATAAN ORISINALITAS

Saya yang bertandatangan di bawah ini:

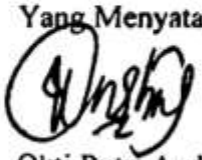
Nama : Okti Putri Andini

NIM : 8111416215

Menyatakan bahwa skripsi yang berjudul "Tinjauan Yuridis Tindak Pidana Cyber terrorism dalam Perpektif Kejahatan Transnasional Terorganisir" adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila dikemudian hari diketahui adanya plagiasi maka saya siap dipertanggungjawabkan secara hukum.

Semarang, 11 Maret 2020

Yang Menyatakan,



Okti Putri Andini

NIM. 8111416215

PERNYATAAN PERSETUJUAN PUBLIKASI

TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Negeri Semarang, saya yang bertanda tangan dibawah ini:

Nama : Okti Putri Andini

NIM : 8111416215

Program Studi : Ilmu Hukum (S1)

Fakultas : Hukum

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Negeri Semarang **Hak Bebas Royalti Noneksklusif** ***(Non-exclusive Royalty Free Right)*** atas skripsi saya yang berjudul :

Tinjauan Yuridis Tindak Pidana *Cyber terrorism* dalam Perspektif Kejahatan Transnasional Terorganisir

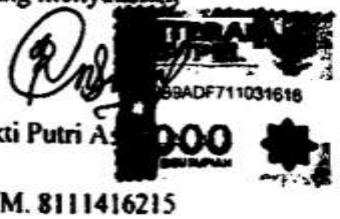
Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Negeri Semarang berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/ pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dnegan sebenarnya.

Dibuat di : Semarang

Pada tanggal : 11 Maret 2020

Yang menyatakan,



Okti Putri A[redacted]

NIM. 8111416215

Motto dan Persembahan

Motto:

"God gives you everything that you want, just not when you want it, but when God knows you need it"

(Allah memberikan apa yang kamu mau, bukan saat kamu menginginkannya, tapi saat Dia tau kamu membutuhkannya)

Persembahan:

Skripsi ini saya persembahkan untuk:

1. Keluarga, Nenek, Orang Tua, Adik, dan Tante, Om beserta Sepupu
2. Almamater Fakultas Hukum Universitas Negeri Semarang
3. Sahabat

PRAKATA

Segala puji bagi Allah SWT yang telah memberikan rahmat dan karunia-Nya, juga junjungan kita Nabi Muhammad SAW sehingga penulis mampu menyelesaikan karya ilmiah skripsi sebagai pemenuhan syarat dalam menyelesaikan studi Strata 1 (S1) di Fakultas Hukum Universitas Negeri Semarang dengan lancar dan baik. Tidak lupa penulis ucapkan terimakasih kepada semua pihak yang telah membantu penulis dalam menjalankan perkuliahan dan akhirnya dapat menyelesaikan penulisan karya ilmiah skripsi, khususnya kepada:

1. Prof. Dr. Fathur Rokhman, M.Hum, Rektor Universitas Negeri Semarang
2. Dr. Rodiyah, S.Pd., S.H., M.Si, Dekan Fakultas Hukum Universitas Negeri Semarang
3. Sonny Saptoajie Wicaksono, S.H., M.Hum, Dosen Pembimbing Skripsi
4. Keluarga tercinta, kakek (alm.) dan nenek, kedua orang tua beserta tante, om, dan sepupu
5. Sahabat- sahabat sejak SMA Ane Maharani, Mufidah, Dione Aufi, Yuan Hasna, serta sahabat saya Yolanda Pusvita dan Ardi Natakusuma
6. Teman- teman Rombel Internasional FH UNNES Angkatan 2016
7. Teman- teman KKN Lokasi Tahap1A Desa Singorojo, Kabupaten Jepara
8. Teman- teman Fakultas Hukum UNNES Angkatan 2016.

Demikian semoga karya ilmiah skripsi saya kelak dapat berguna bagi pengembangan ilmu pengetahuan di Indonesia.

Semarang, 11 Maret 2020

Penulis

ABSTRAK

Andini, Okti Putri. 2020. Tinjauan Yuridis Tindak Pidana *Cyber terrorism* dalam Perpektif Kejahatan Transnasional Terorganisir. Skripsi Bagian Pidana Fakultas Hukum Universitas Negeri Semarang. Dosen Pembimbing: Sonny Saptoajie Wicaksono, S.H., M.Hum.

Kata Kunci: *Cyber terrorism,* Kejahatan Transnasional Terorganisir, Hukum Pidana Internasional

Istilah *Cyber terrorism* muncul dimana sekelompok teroris menggunakan *Cyberspace* dalam melakukan aksi terorisme. Munculnya *Cyber terrorism* sebagai salah satu jenis tindak pidana dan bersifat transnasional tidak diimbangi dengan tersedianya instrument hukum yang dapat menjadi dasar hukum guna mengatasi tindak pidana *Cyber terrorism*. Padahal tindak pidana *Cyber terrorism* bersifat *borderless* dan modus opernadi yang digunakan teroris dalam melakukan tindak pidana *Cyber terrorism* sangat beragam, sehingga target dan cakupan *Cyber terrorism* sangat luas. Berdasarkan hal tersebut instrumen hukum atau pengaturan mengenai tindak pidana *Cyber terrorism* menjadi sangat diperlukan.

Permasalahan yang dibahas dalam penelitian ini adalah mengenai bagaimana pengaturan tindak pidana *Cyber terrorism* dikaji dari perpektif kejahatan transnasional terorganisir. Serta membahas mengenai modus operandi atau bagaimana cara- cara yang dilakukan teroris dalam melakukan tindak pidana *Cyber terrorism*. Tujuan dilakukannya penelitian ini adalah untuk menjelaskan mengenai peraturan apa saja yang mengatur tindak pidana *Cyber terrorism* dari perspektif kejahatan transnasional terorganisir serta menganalisis modus operandi yang digunakan oleh para pelaku tindak pidana *Cyber terrorism.*

Penelitian ini merupakan penelitian hukum normatif dengan menggunakan pendekatan kualitatif dalam menemukan sumber data dengan cara menelaah semua undang- undang dan regulasi yang bersangkutan dengan tindak pidana *Cyber terrorism.* Dikarenakan penelitian ini merupakan penelitian hukum normatif maka sumber data yang digunakan dalam penelitian ini adalah sumber data sekunder. Dalam mengumpulkan data penulis melakukan studi kepustakaan dan validitas data yang didapat diperiksa dengan menggunakan teknik triangulasi. Lalu hasilnya dianalisis dan disajikan menggunakan metode deskriptif analitis.

Hasil dari penelitian ini menemukan bahwa terdapat beberapa konvensi internasional yang dapat digunakan sebagai instrumen hukum pengatur tindak pidana *Cyber terrorism.* Dan berdasarkan kajian yang dilakukan penulis modus operandi yang digunakan oleh teroris dalam melakukan tindak pidana *Cyber terrorism* sangat beragam yaitu melalui peretasan, propaganda, penipuan, serangan *DDoS* dan penyebaran virus, *worm* atau *malware*.

Simpulan yang didapat berdasarkan hasil penelitian ini adalah meskipun belum tersedia instrumen hukum yang mengatur tindak pidana *Cyber terrorism* namun beberapa konvensi internasional yang berkaitan dan telah ada dapat digunakan sebagai instrumen hukum tindak pidana *Cyber terrorism,* dan dapat diketahui bahwa terdapat berbagai macam modus operandi yang digunakan oleh teroris dalam melakukan tindak pidana *Cyber terrorism*.

DAFTAR ISI

Halaman

BAB II : TINJAUAN PUSTAKA

BAB III : METODE PENELITIAN

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi saat ini sangat luas dan tanpa batas, dibalik semua sisi positif yang dapat dimanfaatkan perkembangan teknologi informasi juga menunjukan sisi negatif. Kejahatan- kejahatan yang ditimbulkan internet pun saat ini mencapai dimensi internasional dan transnasional. Istilah kejahatan internasional sendiri merujuk pada suatu peristiwa kejahatan yang sifatnya internasional. Pengertian internasional dalam hal ini adalah pengertian dalam arti luas, meliputi, internasional umum atau global, regional ataupun bilateral dan trilateral. Dengan kata lain kejahatan tersebut dapat menyangkut kepentingan seluruh atau sebagian besar negara di dunia, bahkan kepentingan seluruh umat manusia dapat pula hanya kepentingan negara atau kawasan, atau hanya menyangkut kepentingan dari dua atau lebih negara saja.

Selain itu kejahatan yang ditimbulkan oleh internet juga dapat berdimensi transnasional yang biasa disebut dengan kejahatan transnasional. Kejahatan-kejahatan adalah kejahatan yang pada hakikatnya berdimensi nasional namun memiliki karakteristik transnasional atau lintas negara. *Locus delicti* terjadinya kejahatan transnasional pada kenyataannya masih berada di dalam batas- batas wilayah sebuah negara, namun dalam pelaksanaannya kejahatan transnasional melibatkan urusan- urasan milik negara- negara lain, sehingga seolah- olah terdapat dua atau lebih negara yang memiliki kepentingan terhadap kejahatan tersebut. Jadi inti sebenarnya dari kejahatan transnasional adalah kejahatan tersebut berdimensi

nasional, namun dikarenakan adanya keterkaitan dengan kepentingan negara lain maka tampaklah sifatnya yang transnasional (Parthiana, 2015:46).

Salah satu kejahatan yang berhubungan dengan internet serta memiliki dimensi transnasional adalah kejahatan yang bisa kita sebut dengan istilah *Cybercrime* atau kejahatan melalui jaringan internet. Menurut Kementrian Luar Negeri Republik Indonesia kejahatan *Cybercrime* termasuk dalam kategori kejahatan transnasional, mengingat salah satu ciri khusus kejahatan *Cybercrime* adalah kejahatan ini dilakukan secara *online* dan seringkali tidak dengan jelas dikaitkan ke lokasi geografis manapun, sehingga seringkali melampaui batas- batas negara lain. Dan salah satu ciri kejahatan transnasional adalah dilakukan melampaui batas negara, jadi *Cybercrime* ini sudah memenuhi salah satu syarat untuk disebut sebagai salah satu bagian dari kejahatan transnasional.

Selain alasan tersebut, pada tahun 2010 *Conference of States Parties (CoSP) United Nation Convention Against Transnational Organized Crime (UNTOC)* menyebutkan bahwa terdapat beberapa kejahatan baru yang teridentifikasi sebagai Kejahatan Lintas Negara Baru dan Berkembang *(New and Emerging Crimes)*, kejahatan tersebut antara lain kejahatan dunia maya, kejahatan terkait identitas, penjualan cagar budaya secara gelap, kejahatan lingkungan, perompakan di atas laut, dan perdagangan gelap organ tubuh. Kejahatan Lintas Negara Baru saat ini diberi perhatian khusus oleh dunia internasional dikarenakan angka terjadinya kejahatan tersebut cukup tinggi, kerugian yang ditimbulkan besar serta modus operandi yang digunakan juga sangat beragam.

Cybercrime adalah serangan kriminal yang melibatkan atau terjadi pada *Cyberspace*, wilayah yang sangat halus yang tercipta ketika komputer dan orang

terhubung melalui jaringan elektronik yang membentang di seluruh dunia. *Cybercrime* yang muncul sebagai persoalan kejahatan dan pengadilan internasional merupakan sisi buruk dari masuknya teknologi komunikasi digital, terutama internet, ke dalam kehidupan sehari- hari dan perdagangan global (Natarajan, 2015: 115).

Pengertian *Cybercrime* berkembang terus- menerus secara linear dengan perkembangan kejahatan di internet. Pada mulanya *Cybercrime* hanya mencakup kejahatan *computer crime*, yaitu kejahatan yang ditargetkan pada komputer atau komputer dimanfaatkan sebagai alat guna melakukan kejahatan. Namun saat ini ruang lingkup *Cybercrime* mencakup berbagai kejahatan yang lebih bervariasi dan luas, tidak hanya bentuk *computer crime* saja tetapi juga juga bentuk- bentuk kejahatan lain yang termasuk *computer related crime.*

Dalam *Encyclopedia of cybercrime* dikatakan bahwa:

"*Cybercrime* adalah sebuah istilah yang mencakup semua cara dimana komputer dan jenis perangkat elektronik portable lainnya seperti ponsel dan PDA yang mampu terhubung di internet digunakan untuk melanggar hukum dan menyebabkan kerusakan" (Suseno, 2012:95-96).

Encyclopedia of Cybercrime membagi kejahatan *Cybercrime* dalam beberapa jenis dan salah satunya adalah *Cyber terrorism. Cyber terrorism* adalah kejahatan yang dilakukan oleh oknum yang bermaksud mengedepankan tujuan sosial, agama atau politik namun dengan cara menyebabkan rasa takut yang meluas atau dengan merusak atau menggangu informasi infrastruktur yang penting. (McQuade, 2009:44) Berdasarkan penjelasan jenis- jenis *Cybercrime*, *Cyber terrorism* merupakan kejahatan yang baru muncul. Kejahatan ini menggunakan media

komputer dalam menyebarkan ideologi yang bersifat terror guna menjalankan aksi kejahatan teroris di inetrnet (Astuti, 2015:165).

Internet menyebutkan istilah *Cyber terrorism* sebagai kegiatan dimana sekelompok teroris menggunakan media *Cyberspace* guna melaksanakan aksi terorisme. Jadi *Cyber terrorism* sendiri terdiri dari unsur *Cyberspace* dan terorisme (Gordon, 2006:4). Pengertian *Cyberspace* tidak terbatas kepada dunia yang tercipta akibat dari terjadinya hubungan melalui internet. Internet dapat menyebarkan informasi yang cepat dengan sedikit resiko, serta tidak membutuhkan biaya yang mahal guna melakukan perekrutan yang potensial, sehingga potensi memperoleh partner yang prospektif dalam organisasi teroris menjadi mudah (Seib, 2011:21).

Sedangkan terorrisme dalam penjelasan *Convention of The Organization of the Islamic Confrnece on Combating Internasioanl Terrorism 1999,* merupakan tindakan yang berbentuk kekerasan atau ancaman, yang dilakukan guna menteror orang lain atau memberikan ancaman yang mencelakakan hidup banyak orang, harga diri, kebebasan, keamanan dan hak yang mereka miliki, atau mengeksploitasi harta, sumber daya alam, fasilitas milik pribadi atau publik, atau menguasai, merampas, membahayakan sumber nasional atau fasilitas internasional, atau mengancam stabilitas, integritas territorial, kesatuan politis serta kedaulatan sebuah negara (Dayan, 2015:3).

Jadi dari gabungan pengertian antara *Cyberspace* dan Terrorisme tersebut, Denning berpendapat bahwa *Cyberterrorism* adalah:

“Serangan yang melanggar hukum dan ancaman serangan terhadap komputer, jaringan, dan informasi yang tersimpan di dalamnya ketika dilakukan untuk

mengintimidasi atau memaksa pemrintah atau orang- orangnya untuk melanjutkan politik atau kepentingan sosial.” (Dogrul, 2011:31)

Cyber terrorism melakukan serangan terhadap apa saja yang terhubung dengan internet terutama objek vital milik pemerintah yang dapat menggangu fungsinya bahkan dapat membuat jatuh korban yang lebih besar daripada terorisme dengan modus opernadi konvensional. (Josianto, 2015:165). Negara dituntut untuk mampu menguasai dunia Internet guna mengetahui tindakan teroris dikarenakan *Cyber terrorism* telah menjadi isu dunia. Semakin pesat sebuah teknologi baru berkembang, maka semakin canggih media serta modus opernadi yang digunakan oleh teroris sehingga semakin besar kesempatan tindak pidana terorisme bisa terjadi.

Menurut *United Nations Office on Drugs and Crime* (UNODC) dalam penelitiannya yang dirangkum dalam sebuah diagram dibawah ini, sebanyak 7% negara anggota UNODC sepakat bahwa *Cyber terrorism* merupakan salah satu kejahatan yang dianggap memiliki pengaruh kerusakan yang cukup besar apabila menimpa suatu negara.

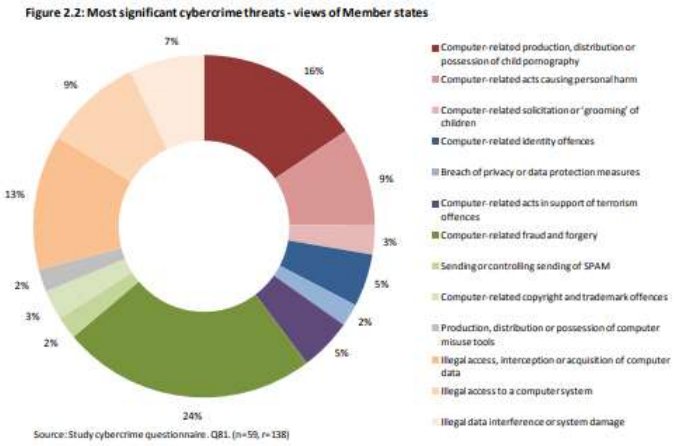


Diagram 1.1 Jenis kejahatan siber yang paling signifikan menurut negara anggota UNODC. Sumber: *United Nations Office on Drugs and Crime* (UNODC).

Menurut data yang penulis kumpulkan bahwa sejak tahun 1996 sampai dengan tahun 2019 sudah terjadi kurang lebih 17 kasus di dunia yang merupakan salah satu bentuk dari *Cyber terrorism* dengan berbagai macam cara dan sasaran. Menurut Enver Bucaj dalam penelitiannya disimpulkan bahwa, tingginya angka *Cyber terrorism* ini sampai sekarang tidak diimbangi dengan adanya regulasi khusus yang dapat digunakan untuk mengatasi tindak pidana *Cyber terrorism* secara global. Padahal menetapkan dasar hukum secara global untuk melawan *Cyber terrorism* sangatlah penting (Bucaj, 2017:160).

Berbagai bentuk tindak pidana yang digunakan sebagai modus operandi yang digunakan teroris dalam melakukan tindak pidana *Cyber terrorism* juga menjadi salah satu alasan mengapa perlu adanya regulasi khusus guna penegakan tindak pidana *Cyber terrorism*. Salah satu cara atau modus operandi yang digunakan oleh teroris dalam melakukan tindak pidana *Cyber terrorism* adalah penyebaran propaganda, hukum nasional maupun hukum internasional belum mengatur mengenai kejahatan penyebaran propaganda tersebut, padahal efek dari kejahatan propaganda tersebut cukup besar dan berpengaruh bagi kehidupan sebuah negara. Apabila regulasi mengenai salah satu bentuk *Cyber terrorism* tersebut belum tersedia, maka akan menyulitkan sebuah negara dalam hal penegakan kejahatannya.

Pentingnya regulasi mengenai *Cyber terrorism* juga tidak hanya disebabkan karena belum adanya regulasi khusus yang mengatur tindak pidana tersebut, namun juga dikarenakan posisi tindak pidana *Cyber terrorism* yang merupakan salah satu

bentuk dari kejahatan transnasional terorganisir. Menurut Rahmani Dayan dalam bukunya, terdapat karakteristik khusus yang dimiliki oleh terorisme namun tidak dimiliki oleh kejahatan- kejahatan konvensional lain, tindak pidana tersebut dilakukan secara terstuktur dan melebar serta terorganisasi sehingga menjadi sebuah ancaman yang sangat serius bagi masyarakat, bangsa dan negara. Oleh karena itu *Cyber terrorism* termasuk dalam kategori "*Transnational Organized Crime"* (Dayan, 2015:12).

Luasnya cakupan dari kasus *Cyber terrorism* ini membuat hukum nasional negara- negara yang bersangkutan tidak akan cukup untuk menyelesaikan kasus *Cyber terrorism*. Selain itu masuknya tindak pidana *Cyber terrorism* kedalam kategori kejahatan transnasional terorganisir ini membuat pengaturan yang mengatur tindak pidana ini harus lebih banyak. Maka dari itu penulis ingin mengkaji tindak pidana *Cyber terrorism* ini dari perspektif kejahatan transnasional terorganisir, agar dapat menjelaskan mengenai peraturan apa saja yang bisa menjadi dasar hukum tindak pidana ini, serta menemukan modus operandi yang dilakukan oleh teroris dalam melancarkan aksi ternya.

1.2 Identifikasi Masalah

Latar belakang masalah tersebut membuat penulis mengidentifikasi beberapa permasalahan yang dapat diteliti, permasalahan tersebut adalah sebagai berikut:

1. Bahwa pengaturan mengenai tindak pidana Kejahatan Transnasional Terorganisir khususnya *Cyber terrorism* belum secara spesifik ada dalam perkembangan Hukum Pidana Internasional

2. Bahwa munculnya tindak pidana *Cyber terrorism* ini terjadi dikarenakan munculnya banyak ide- ide baru yang dimiliki para kelompok teroris untuk melancarkan aksi terornya.

1.3 Pembatasan Masalah

Berdasarkan permasalahan yang diidentifikasi oleh penulis diatas maka penulis menetapkan pembatasan masalah sebagai upaya untuk memfokuskan penelitian skripsi ini. Masalah yang akan dibahas pada skripsi ini adalah:

1. Pengaturan dalam Hukum Pidana Internasional mengenai tindak pidana *Cyber terrorism* sebagai dalah satu bentuk dari Kejahatan Transnasional Terorganisir.
2. *Modus Operandi* para *Cyber terrorist* dibalik tindak pidana *Cyber terrorism*

1.4 Rumusan Masalah

Mengacu pada latar belakang masalah tersebut maka permasalahan yang akan diteliti dan dituliskan dalam penelitian ini adalah :

1. Bagaimana pengaturan tindak pidana *Cyber terrorism* ditinjau dari perspektif Kejahatan Transnasional Terorganisir*?*
2. Bagaimanakah modus operandi tindak pidana *Cyber terrorism?*

1.5 Tujuan Penelitian

Tujuan yang ingin dicapai oleh penulis setelah melakukan penelitian adalah:

1. Untuk menganalisis mengenai peraturan yang mengatur tindak pidana *Cyber terrorism* dari perspektif Kejahatan Transnasional Terorganisir.
2. Untuk menemukan dan menjelaskan modus operandi yang digunakan oleh para pelaku tindak pidana *Cyber terrorism*.

1.6 Manfaat Penelitian

Manfaat yang ingin diberikan oleh penulis setelah melakukan penelitian ini adalah:

1. Secara Teoritis, peneliti berharap hasil penelitian ini mampu menambah pengetahuan dan pemikiran yang bermanfaat bagi penegakan Hukum Pidana khususnya Hukum Pidana Internasional.
2. Secara Praktis, bagi peneliti, penelitian ini dapat memberi informasi dan wawasan mengenai pengaturan tindak pidana *Cyber terrorism* dari prespektif Kejahatan Transnasional Terorganisir.

BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian dalam skripsi ini merupakan penelitian yang orisinil dan dapat dipertanggung jawabkan oleh penulis. Penulisan penelitian ini murni ide dan pemikiran penulis sendiri, dengan bantuan studi komparatif penelitian lain yang berbeda obyek dan subyek penelitiannya. Namun untuk mendukung kevaliditasan penelitian ini penulis mengkomparasikan dengan beberapa penelitian yang relevan serta terdahulu yang telah ada, penelitian tersebut adalah:

No	Nama Pengarang dan Judul	Hasil Penelitian	Perbedaan
1.	*"Analisis Instrumen Cyber terrorism dalam Kerangka Sistim Hukum Internasional"* oleh Alfira Nurliliani Samad, Universitas Hasanudin Makasar.	Adapun hasil dari penelitian tersebut menyimpulkan bahwa tindak pidana *Cyber terrorism* tidak termasuk dalam kejahatan internasional namun termasuk dalam bentuk kejahatan transnasional. Serta disimpulkan bahwa meskipun belum ada	Perbedaan antara skripsi tersebut dan skripsi ini adalah penulis skripsi tersebut meninjau tindak pidana *Cyber terrorism* dari sudut pandang hukum internasional,

		pengaturan yuridis di hukum internasional yang mengatur mengenai tindak pidana *Cyber terrorism* namun ada beberapa konvensi internasional yang dapat digunakan sebagai acuan sumber hukum penanganan tindak pidana *Cyber terrorism.*	sedangkan penulis meninjau *Cyber terrorism* dari sudut pandang tindak pidana transnasional terorganisir.
2.	"*Pengaturan Tindak Pidana Terorisme dalam Dunia Maya (Cyber terrorism) Berdasarkan Hukum Internasional"*. Oleh Ari Maharta, Universitas Udayana Bali	Penelitian ini membahas menganai dua hal yaitu mengenai instrument hukum pengaturan *Cyber terrorism* berdasarkan hukum internasional dan bagaimana harmonisasi pengaturan mengenai *Cyber terrorism* antara hukum nasional di Indonesia dengan instrument hukum internasional.	Adapun perbedaan antara penelitian ini dengan skripsi penulis terletak pada sudut pandang tinjauan penelitian. Dalam skripsi diatas *Cyber terrorism* ditinjau dari sudut pandang hukum internasional,

		Hasil yang dapat disimpulkan oleh peneliti dalam penelitian ini adalah bahwa terorisme *Cyber terrorism* dikatgorikan sebagai salah satu kategori kejahatan transnasional terorganisir bukan sebagai bentuk dari kejahatan internasional serta belum terdapat satupun instrument hukum internasional yang meregulasi *Cyber terrorism* secara khusus . Namun guna mengisi kevakuman hukum, *ASEAN Convention on Counter Terrorism dan Internasional Convention for the Suppression of Terrorist Bombings* dapat dipergunakan sementara.	sedangkan penulis meninjau dari sudut kejahatan transnasional terorganisir.

		Namun tetap sangat penting untuk melakukan pembentukan peraturan hukum internasional mengenai hal tersebut. Selain itu penulis juga menyimpulkan bawa upaya harmonisasi pengaturan hukum mengenai *Cyber terrorism* ini amat sangat penting untuk dilakukan. Serta sangat penting dilakukan pembentukan peraturan hukum nasional mengenai *Cyber terrorism*.	

2.2 Landasan Teori

Teori kebijakan hukum pidana biasa juga dikenal sebagai politik hukum pidana. Sudarto dalam bukunya menyebut bahwa dalam pelaksanaan politik hukum pidana artinya kita sedang menyelenggarakan suatu pemilihan guna menciptakan hasil yang baik dalam merumuskan sebuah perundang- undangan, perundang- undangan yang baik berarti bahwa perundang- undangan tersebut telah menjadi perundangan yang memiliki daya guna serta keadilan karena dua

hal tersebut merupakan syarat yang harus dipenuhi (Sudarto, 1981:159). Disini berarti bahwa makna pelaksanaan politik hukum pidana adalah bagaimana memaksimalkan dalam hal pembuatan dan perumusan suatu hukum atau undang- undang agar dilakukan secara maksimal dan menghasilkan hasil yang baik.

Melaksakanan kebijakan dengan usaha guna membentuk peraturan hukum yang berkualitas pada dasarnya merupakan salah satu tujuan penanggulangan kejahatan. Ini berarti bahwa politik kriminal menjadi induk dari pelaksanaan kebijakan atau politik hukum pidana. Dinilai dari sisi politik kriminal, politik hukum pidana memiliki makna yang sama dengan kebijakan yang dibuat guna menanggulangi tindak kejahatan dengan menggunakan hukum pidana. Selain itu hakikat dari usaha menanggulangi kejahatan menggunakan hukum pidana sebenarnya merupakan salah satu tujuan dari usaha penegakan hukum terutama dalam hukum pidana. Maka dari itu sering kali dianggap bahwa kebijakan atau politik hukum pidana merupakan bagian dari kebijakan penegakan hukum.

Pembuatan kebijakan atau perundang- undangan guna penanggulangan kejahatan merupakan bagian integral dari usaha dalam hal perlindungan masyarakat. Hal tersebut menunjukan bahwa kebijakan atau politik hukum pidana juga merupakan bagian dari kebijakan atau politik sosial. Ini berarti bahwa tujuan utama dari pembuatan kebijakan atau politik hukum pidana merupakan sebuah usaha untuk melindungi masyarakat guna mencapai kesejahteraan masyarakat. Kebijakan atau politik hukum dalam hal ini menlingkupi bidang hukum materil, formil dan pelaksanaan pidana (Arief, 2008:28).

2.3 Landasan Konseptual

Kumpulan beberapa hal yang ememilik arti yang berkaitan lalu digambarkan dalam bentuk konsep- konsep khusus, dengan istilah yang menajadi obyek penelitian dan/atau yang akan dijabarkan dalam sebuah karya ilmiah (Ali, 2013:96). Landasan konseptual berisi mengenai kegiatan menemukan sebuah landasan pengertian dan landasan operasional guna melaksanakan sebuah penelitian dengan cara mengkaji teori- teori serta definisi- definisi tertentu (Waluyo, 2002:30). Adapun konseptual yang digunakan dalam penulisan usulan skripsi ini adalah sebagai berikut:

2.3.1 Terorisme

2.3.1.1 *Definisi Terorisme*

Definisi mengenai terrorisme pada dasarnya kontroversial dikarenakan terdapat kesulitan dalam pendefinisiannya sehingga terdapat beberapa pendapat yang dikeluarkan oleh lembaga pemerintah yang terkait dengan penegakan tindak pidana terrorisme. Definisi tersebut adalah:

Majelis Umum PBB pada 1994 menggambarkan tindak pidana terrorisme sebagai tindak kriminal yang ditujukan atau diperkirakan akan berhasil menciptakan keadaan terror di masyarakat umum melalui tindak provokasi, oleh sekelompok orang atau indovidu tertentu untuk tujuan politik, yang tidak dapat dibenarkan dengan alasan apapun yakni apa pun pertimbangan politiknya, filosofis, ideologis, ras, etnis, agama atau sifat lain, apa pun yang dapat digunakan untuk membenarkan mereka.

Konvensi Arab untuk Penindasan Terorisme diadopsi oleh Dewan Menteri Dalam Negeri Arab dan Dewan Menteri Kehakiman Arab di Kairo, Mesir pada tahun 1998. Terrorisme didefinisikan dalam konvensi sebagai setiap kegiatan pengancaman ataupun kekerasan,dengan menggunakan motif atau tujuan apa pun, yang terjadi guna mengedepankan agenda individu atau kriminal kolektif dan berusaha menyebarkan kepanikan banyak orang, menciptakan ketakutan dengan melukai mereka, atau membuat hidup, kebebasan atau rasa aman yang harusnya mereka miliki menjadi dalam bahaya, atau berusaha untuk menyebabkan kerusakan pada lingkungan atau untuk instalasi atau property public atau pribadi atau untuk menduduki atau merebutnya, atau berusaha untuk membahayakan sumber daya nasional.

Resolusi Dewan Keamanan PBB 1566 (2004) memberikan definisi bahwa terrorisme merupakan tindakan kriminal, berikut ditargetkan terhadap warga sipil, yang dilakukan dengan tujuan untuk membuat kematian atau cedera serius terhadap tubuh manusia atau melakukan tindakan penyandraan, dengan tujuan guna menciptakankeadaan terror di masyarakat umum atau dalam sekelompok orang atau orang- orang tertentu dengan memprovokasi, menakut- nakuti penduduk atau memaksa pemerintah atau organisasi internasional untuk melakukan atau tidak melakukan tindakan apapun.

Federal Bureau of Investigation (FBI) mendefinisikan terorisme sebagai kekerasan terhadap orang dan/atau properti secara tidak sah guna

mengancam atau memaksa suatu pemerintahan, penduduk sipil, atau bagian daripadanya, yang mengedepankan kemajuan tujuan politik atau sosial.

Hoffman16 mengidentifikasi beberapa elemen kunci terorisme dengan membedakan teroris dari jenis penjahat lain dan terorisme dari bentuk kejahatan lainnya, kita menjadi sadar bahwa terorisme adalah

- Tujuan dan motif politik yang tak terhindarkan
- Kekerasan atau sama pentingnya, mengancam kekerasan
- Direncanakan guna menciptakan dampak psikologis yang luas diluar korban atau target langsung
- Dilakukan oleh sekelompok orang dengan strukturisasi yang dapat diidentifikasi atau organisasi tidak resmi (yang anggotanya tidak mengenakan seragam atau mengidentifikasi lencana) dan
- Dilakukan oleh kelompok sub nasional atau entitas non- negara.

2.2.1.2. Penyebab Terorisme

United States Intitute of Peace (2001:10) telah mengkategorikan beberapa motivasi yang menyebabkan dilakukannya tindak pidana terorisme, motivasi tersebut dilihat dari tiga perspektif, yaitu:

(1) Perspektif Psikologis

Mereka yang terlibat dalam terorisme dapat melakukannya semata-mata karena alasan pribadi, berdasarkan keadaan psikologis mereka sendiri. Motivasi mereka mungkin tidak lebih dari kebencian atau keinginan akan kekuasaan. Dalam banyak hal, teroris tertarik untuk

mendapatkan perhatian dari orang lain atas tindakannya, daripada beberapa tujuan besar ideologis atau strategis.

(2) Perspektif Ideologis

Perspektif Ideologi didefinisikan sebagai kepercayaan, nilai- nilai dan atau prinsip- prinsip yang dengannya suatu kelompok mengidentifikasi maksud dan tujuannya. Ideologi dapat mencakup filosofi dan program agama atau politik.

(3) Perspektif Strategis

Perspektif strategis dipandang sebagai perpanjangan logis dari kegagalan politik. Ketika orang mencari penyelesaian atas eluhan mereka melalui pemerintah, tetapi gagal memenangkan perhatian pemerintah terhadap penderitaan mereka, mereka mungkin menggunakan kekrasan. Dari sudut pandang ini, terorisme adalah hasil analisis logis dari tujuan dan sasaran kelompok, dan perkiraan mereka tentang kemungkinan mendapatkan kemenangan. Jika kemenangan tampaknya tidak mungkin menggunakan cara oposisi yang lebih tradisional, maka orang dapat menghitung bahwa terorisme adalah pilihan yang lebih baik.

2.2.1.3.Jenis- jenis Terorisme

Para pakar era modern mendefinisikan dan menggambarkan terorisme dalam konteks klasifikasi tipologis sistematis, pembagian jenis terorisme tersebut berbeda berdasarkan motif ataupun media yang digunakan. Pembagian jenis terorisme berdasarkan motivasi yang ingin dicapai adalah sebagai berikut:

(1) Terorisme Baru: lingkungan teroris modern yang muncul pada akhir abad ke-20 yang memuncak pada serangan teroris 11 september di New York City. Terorisme baru dicirikan sebagai ancaman serangan korban massal dari organisasi teroris pembangkang, konfigurasi organisasi teroris baru dan kreatif, solidaritas keagamaan transnasional dan pembenaran moral yang didefinisikan ulang untuk kekerasan politik.

(2) Terorisme Negara: terorisme yang dilakukan pemerintah terhadap musuh yang dimiliki. Terorisme negara dapat diarahkan secara eksternal terhadap musuh di dimain internasional atau secara internal melawan musuh domestik.

(3) *Dissident Terrorism:* terorisme yang dilakukan oleh gerakan dan kelompok non- negara terhadap pemerintah, kelompok etnis, kelompok agama, dan musuh yang dianggap lainnya.

(4) Terrorism Agama: terorisme yang dimotivasi oleh keyakinan mutlak bahwa kekuatan dunia lain telah menyetujui dan memerintahkan penerapan kekerasan teroris untuk kemuliaan iman yang lebih besar. Terorisme keagamaan biasanya dilakukan untuk membela apa yang orang percaya dan orang anggap sebagai satu-satunya iman yang benar.

(5) Terorisme Ideologis: terorisme dimotivasi oleh sistem kepercayaan politik (ideologi), yang memperjuangkan hak- hak inheren yang dirasakan sendiri dari suatu kelompok tertentu atau kepentingan yang bertentangan dengan kelompok atau kepenting lain. Sistem

kepercayaan menggabungkan pembenaran teoretis dan filosofis karena secara tegas menegaskan hak- hak kelompok atau kepentingan yang diperjuangkan.

(6) Terorisme Internasional: terorisme yang merambah ke panggung dunia. Target dipilih karena nilainya sebagai simbol kepentingan internasional, baik di dalam negara asal atau melintasi betas negara.

Pembagian jenis terorisme berdasarkan dengan jenis serangan atau media yang dilakukan oleh teroris:

(1) Bioterrorism

Bioterrorism menggunakan racun biologis untuk menyakiti dan menakut- nakuti warga yang tidak bersalah, ats nama alasan politik atau lainnya. Pusat Pengendalian Penyakit A.S telah mengkategorikan virus, bakteri, dan racun yang dapat digunakan dalam serangan, mereka adalah Anthrax *(Bacillus anthracis)*, Botulisme *(Clostridium botulium)*, Wabah *(Yersinia pestis)*, Cacar *(Variola mayor)*, Tularemia *(Francisellatularensis)*, Demam *hemorrahagik* (karena Virus Ebola atau Virus Marburg).

(2) Cyber terrorism

Teroris memanfaatkan teknologi informasi untuk mempengaruhi masyarakat luas dan mendapatkan perhatian pada tujuan mereka. Mereka menggunakan teknologi informasi, seperti telekomunikasi, komputer dan internet, sebagai alat untuk mengatur serangan konvensional. Dalam terorisme *cyber*, dengan menggunakan

teknologi informasi akan secara radikal mengganggu layanan yang terhubung dengan internet. Sebagai contoh, teroris dunia maya dapat meretas jaringan perumahan untuk mendapatkan informasi keuangan kritis atau menonaktifkan sistem darurat jaringan. *Cyber terrorism* adalah penggunaan internet untuk kegiatan teroris sperti gangguan besar- besaran jaringan komputer, terutama komputer yang terhubung ke internet, dengan cara virus komputer.

(3) Ecoterrorism

Ecoterrorism berarti penggunaan kekerasan dan terror oleh kelompok radikal yang berorientasi lingkungan untuk mencegah pemerasan dan penjarahan lingkungan. *Ecoterrorism* bertujuan untuk menarik perhatian public untuk memperlambat ekspolitasi sumber daya alam, kerusakan habitat, dan pemotongan pohon yang tidak berkelanjutan. Dalam hal ini *Ecoterrorism* mencakup "pembangkangan sipil" dan "aktivisme politik" dna tidak menargetkan orang tetapi properti dan institusi yang merusak lingkungan. Front Pembebasan Bumi *(ELF)* Front dan Pembebasan Hewan *(ALF)* dianggap sebagai perwakilan modern dari *Ecoterrorism (*Gungormez, 2019:10).

(4) Nuclearterrorism

Terorisme nuklir dapat didefinisikan sebagai Tindakan terorisme di mana seseorang atau kelompok organisasi meledakan perangkat nuklir. Ini juga dapat didefinisikan sebagai sabotase fasilitas nuklir dan/ atau peledakan perangkat radiologis. Secara hukum terorisme

nuklir adalah pelanggaran yang dilakukan jika seseorang secara tidak sah dan sengaja menggunakan bahan radioaktif apa pun dengan maksud untuk menyebabkan kerusakan substansial pada property atau lingkungan, atau dengan niat untuk memaksa orang alami atau hukum, organisasi internasionalatau negara untuk melakukan atau menahan diri dari melakukan sebuah Tindakan (Ndikilar, 2019:4).

(5) Narcoterrorism

Narcoterrorism dapat merujuk berbagai situasi, termasuk kekerasan yang dilakukan oleh penyelundup narkoba dan taktik teroris oleh actor negara, penggunaan perdagangan narkoba atau kegiatan terkait langsung dan tidak langsung oleh organisasi teroris untuk mendanai operasi mereka, kerjasama antara pengedar narkoba dan organisasi teroris untuk keuntungan Bersama, dan penggabungan organisasi-organisasi perdagangan obat- obatan terlarang dan organisasi-organisasi teroris untuk melakukan kegiatan- kegiatan perdagangan narkoba dan teroris (Gomis, 2015:3).

2.3.2 *Cybercrime*

2.3.2.1 Definisi Cybercrime

Istilah *"Cybercrime*" memiliki arti yang sama atau sinonim dengan beberapa kata, diantaranya: *technological crime, high technology crime, high tech crime, economic crime, internet crime, digital crime,* atau *electronic crime,* sinonim tersebut merupakan beberapa kata lain yang digunakan guna penggambaran kejahatan yang dilakukan dengan komputer

atau teknologi informasi lainnya oleh orang- orang (McQuade, 2009:44). Namun sebenarnya *Cybercrime* adalah istilah luas yang melingkupi keseluruhan cara yang digunakan saat komputer dan jenis perangkat elektronik portabel lainnya seperti ponsel dan PDA yang memiliki kapasitas terhubung dengan Internet, digunakan untuk melanggar hukum dan menyebabkan kerugian.

Definisi teknis dari *Cybercrime* adalah dimana komputer atau perangkat elektronik lainnya digunakan guna memfasilitasi perilaku illegal melalui sistem informasi seperti jaringan organisasi atau internet (McQuade, 2006:16). Menurut Kamus Besar Bahasa Indonesia *Cybercrime* adalah tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. Pemanfaatan perkembanagan teknologi komputer khususnya internet yang dilakukan secara salah menyebabkan munculnya kejahatan *Cybercrime*. Internet menghadirkan *Cyberspace* dan menawarkan kepada manusia berbagai harapan dan kemudahan dengan realitas virtual yang dimilikinya. Akan tetapi dibalik itu, timbul sebuah persoalan berupa perbuatan hukum yang lebih mengarah pada kejahatan yang disebut dengan *Cybercrime*, dalam kejahatan tersebut sasaran targetnya adalah sistem jaringan komputernya itu sendiri yang digunakan untuk melakukan aksi kejahatan dunia maya. Terminologi *Cybercrime* sendiri memliki pengertian yang berbeda- beda menurut beberapa literature dan ahli. Menurut Thomas and Loader mereka berpendapat bahwa *Cybercrime* adalah aktivitas yang menggunakan media komputer yang

illegal atau dianggap illegal oleh pihak- pihak terstentu dan yang dapat dilakukan melalui jaringan elektronik global (Sigid Suseno, 102: 92).

Menurut *United Nation Office on Drug and Crime*:

"*Cybercrime* adalah bentuk kejahatan transnasional yang terus berkembang. Sifat kompleks kejahatan ini sebagai kejahatan yang terjadi didunia maya tanpa dibatasi oleh batas meningkatkan keterlibatan kelompok kejahatan terorganisir. Pelaku kejahatan dunia maya dan korbannya dapat ditemukan diberbagi wilayah, dan dampaknya dapat beriak di masyarakat di seluruh dunia, menyoroti perlunya meningkatkan respons mendesak, dinamis, dan internasional."

Menurut *The Council of Europes Cybercrime Treaty* menggunakan terminologi *Cybercrime* untuk merujuk pada:

"tindakan pelanggaran mulai dari aktivitas kriminal terhadap data hingga konten dan pelanggaran hak cipta"

Sedangkan Zeviar Geese dan *The United Nations Manual on the Prevention and Control of Computer Ralated Crime* menginginkan definisi yang lebih luas lagi yaitu dengan memasukan penipuan, pengaksesan secara tidak sah, pornografi anak, *cyberstalking*, dan pemalsuan kedalam definisi *Cybercrime* (Gordon, 2006:2).

Selain itu *Organization for economic cooperation development* (OECD) juga memberikan pengertian bahwa *Cybercrime*

"any unauthorized, unethical or not based on sufficient authority, which involves automatic data processing and data transmission, where the definition also includes economic crimes related to cimputers, violations of individual privacy related to computers, and violations of national security policies."

2.3.2.2 Karakteristik Cybercrime

Selain dapat dimengerti dari pengertiannya, *Cybercrime* juga dapat diketahui dari karkteristik, menurut David L Speer *Cybercrime* memiliki beberapa karakteristik:

(1) Tidak terbatas atau melampaui waktu, ruang, dan tempat, juga dapat disebut memiliki batasan- batasan yang tidak tegas, melampaui atau melintasi sejumlah yurisdiksi dan terjadi seketika;

(2) Belum diatur dalam seperangkat instrument hukum yang baku dan tegas yang dapat menajdi landasan dalam masyarakat umum bertindak, ajdi sifatnya masih sangat lentur;

(3) Perihal usaha penegakan hukumnya kejahatan tersebut mensyaratkan perlunya pengetahuan teknis yang memadai, pengetahuan yang umumnya diperoleh dari pendidikan tinggi;

(4) Tidak tersedianya kesepakatan atau nilai- nilai yang tegas mengenai apa yang mencakup atau tidak tercakup kedalam pengertian tindak pidana *Cyber;*

(5) *Cybercrime* cenderung berbentuk pelanggaran yang tidak memiliki tingkatan parah yang cukup besar dan dalam pelaksanaanya tidak terfokus pada korban serta pelanggar hukum biasanya merupakan individu yang bekerja sendiri.

Pada tahun 2011 *The Council of Europe (CoE)*, mengadaptasi *Convention on Cybercrime* yang lebih dikenal dengan *Budapest Convention*

yang mengidentifikasi beberapa kegiatan yang termasuk sebuah kejahatan di dunia maya, antara lain:

- Dengan sengaja tanpa hak mengakses seluruh bagian dari semua sistem komputer
- Dengan sengaja tanpa hak melakukan penangkapandari transmisi data komputer pribadi atau *non- public*
- Dengan sengaja tanpa hak melakukan pengrusakan, penghapusan, perubahan, atau penindasan data komputer.
- Dengan sengaja dan secara serius menghalangi fungsi sistem komputer melalui pemasukkan, pentransmisian, perusakan, penghapusan, sampai memperburuk, mengubah, atau menekan data komputer.
- Melakukan kegiatan produksi, penjualan, pengadaan yang untuk digunakan untuk mengimpor, atau mendistribusikan perangkat yang dirancang untuk melakukan kajahatan, atau kata sandi dan data serupa yang digunakan untuk mengakses sistem komputer, dengan maksud melakukan kejahatan yang disebutkan diatas.

2.3.2.3 Jenis- Jenis Cybercrime

Cybercrime sendiri yang utama dapat dikategorikan dalam dua kategori:

(1) Menggunakan komputer sebagai target;

Berarti menggunakan komputer untuk menyerang computer lain. Misalnya melakukan peretasan, serangan *virus/ worm*, serangan DOS, dll

(2) Menggunakan komputer sebagai senjata.

Berarti menggunakan komputer untuk melakukan kejahatan dunia nyata. Misalnya terorisme dunia maya, pelanggaran hak kekayaan intelektual, penipuan kartu kredit, penipuan EFT, pornografi, dll (Vadza, 2013:130)

(3) *The UK law Enforcement Agencies* menambahkan satu lagi kategori *Cybercrime* yaitu menggunakan computer sebagai fasilitator perantara. Misalnya ketika penjahat menggunakan komputer untuk kegiatan yang terkait dengan kejahatan, tetapi tidak dalam dirinya criminal, seperti melakukan perncanaan dan penelitian.

Sebagai media, komputer dapat berfungsi sebagai modus operandi kriminal, dan sebagai perantara, sistem komputer bertindak sebagai penyangga antara pelanggar dan korbannya, yang mempengaruhi cara suatu pelanggaran dilakukan atau dieksekusi. Sebagai fasilitator komputer memungkinkan komunikasi antara pelaku diruang yang dapat diakses secara global yang relatif cepat. Ketika komputer bertindak sebagai media yang menyinggung, kontak pelaku/ konspirator harus dipertimbangkan, sedang ketika bertindak sebagai fasilitator yang menyinggung, ia membantu kontak antara pelaku (Jahankhani: 153).

2.3.3 *Cyber terrorism*

Barry Collin, *researcher* di *Institute for Security and Intelligence in California*, menciptakan istilah "*Cyber terrorism"* pada 1980-an. Konsep ini terdiri dari dua elemen, yaitu: elemen dunia maya dan terorisme.

Cyberspace dapat dianggap sebagai tempat dimana program komputer berfungsi dan tempat bergeraknya data (Collin, 1996).

Pada 1990 *National Academy of Science* memulai laporan tentang keamanan computer dengan kalimat "Kami sedang dalam resiko. Semakin lama, Amerika tergantung pada komputer. Besok, teroris mungkin dapat melakukan lebih banyak kerusakan dengan menggunakan keyboard daripada bom". Pada saat itulah diciptakan istilah *"pearl harbor elektronik"*, yang menghubungkan ancaman serangan komputer dengan sejarah Amerika. Dari perspektif psikologis, dua ketakutan terbesar di zaman modern ini digabungkan dalam istilah "*Cyber terrorism"* (Weimann, 2004:3). Seperti halnya *Cybercrime*, *Cyber terrorism* juga memiliki banyak definisi yang berbeda, antara lain:

James Lewis, mendifinisikan *Cyber terrorism* sebagai penggunaan jaringan computer dunia maya dan alat internet untuk memecah infrastruktur nasional yang kritis (seperti energy, angkutan umum, kegiatan pemerintah, dll), atau bisa juga untuk mengintimidasi atau memaksa pemerintah suatu negara atau warganegaranya (Vilic, 2017:69).

Cambridge Center for Risk Studies mendefinisikan:

"Terorisme dunia maya sebagai tindakan kekerasan bermotivasi politik yang melibatkan kerusakan fisik atau cedera pribadi yang disebabkan oleh gangguan digital jarak jauh dengan sistem teknologi."

Selain itu Dorothy Denning, seorang *professor of computer science*, telah mengajukan definisi yang sangat jelas dalam banyak artikel dan dalam

kesaksiannya tentang masalah ini dihadapan *The House Armed Services Committee* pada Mei 2000, bahwa:

"*Cyber terrorism* adalah konvergensi dunia maya dan terorisme. Ini merujuk pada serangan yang melanggar hukum dan nacaman terhadap komputer, jaringan, dan informasi yang tersimpan di dalamnya ketika dilakukan untuk mengintimidasi atau memaksa pemerintah atau orang-orangnya untuk meningkatkan tujuan politik atau sosial."

Selanjutnya, untuk memenuhi syarat sebagai *Cyber terrorism*, serangan harus menghasilkan kekerasan terhadap orang atau properti, atau setidaknya menyebabkan cukup banyak bahaya dan menimbulkan ketakutan. Serangan yang menyebabkan kematian atau cedera tubuh, ledakan atau kerugian ekonomi yang parah akan menjadi contoh. Serangan serius terhadap infranstruktur kritis dapat menjadi tindakan "*Cyber terrorism"* tergantung pada dampaknya. Serangan – serangan yang merupakan gangguan yang mahal tidak akan terjadi pada tindak pidana ini.

Federal Bereau of Investigation (FBI) menggambarkan *Cyber terrorism* sebagai pengembangan kemampuan teroris yang disediakan oleh teknologi baru dan organisasi jaringan, yang memungkinkan teroris untuk melakukan operasi mereka dengan sedikit atau tanpa risiko fisik untuk diri mereka sendiri" yang difokuskan pada "penghancuran fisik perangkat keras dan perangkat lunak informasi, atau kerusakan fisik untuk personel atau peralatan yang menggunakan teknologi informasi sebagai media (Vilic, 2017:70).

Definisi terakhir dari *Cyber terrorism* ini dapat dianggap sebagai:

"Penggunaan terencana dari kegiatan yang mengganggu, atau ancaman dengan target komputer dan/atau jaringan, yang bermaksud untuk menyebabkan kerusakan atau tujuan sosial, ideologis, agama, politik atau hal serupa, atau untuk mengintimidasi siapa pun dalam kemajuan lebih lanjut. dari tujuan tersebut."

Cybercrime termasuk pelanggaran jaringan yang tidak sah dan pencurian kekayaan intelektual dan data lainnya; ini dapat dimotivasi secara finansial, dan respons biasanya merupakan yurisdiksi lembaga penegak hukum (Theohary, 2015).

Dengan demikian, dapat ditarik garis tengah bahwa *Cyber terrorism* merupakan tindakan yang melibatkan kegiatan aktif maupun pasif. Aktif berarti menggunakan komputer untuk melakukan infiltrasi terhadap infrastruktur penting dalam negara, seperti listrik, layanan darurat, telekomunikasi, suplai air, ekonomi, militer, dan institusi finansial sebuah negara yang bisa berakibat fatal. Sisi pasif menunjukkan bahwa *Cyber terrorism* juga dapat melakukan rekrutmen, mencari dukungan, dan melakukan propaganda dengan tujuan untuk menyebarkan rasa takut kepada masyarakat global di dunia maya (Widiyanto, 2017:176).

Menurut *DCSINT Handbook No.1.02, Cyber operations and Cyber terrorism,* yang digunakan untuk melatih tantara AS, operasi internet terdiri dari terorisme internet dan dukungan internet, diekspresikan melalui perencanaan, rekrutmen dan propaganda. Dengan aktivitas semacam ini, jaringan computer dapat digunakan sebagai senjata, sebagai target perantara atau sebagai aktivitas yang mendahului atau mengikuti serangan fisik. *The Manual* menyatakan bahwa tujuan paling penting dari *Cyber terrorism* adalah hilangnya integritas target itu sendiri, mengurangi kemungkinan tindakannya, kurangnya kepercayaan, keamanan, dan keselamatan, dan akhirnya kehancuran fisik. Motivasi paling umum yang diidentifikasikan dalam *Cyber terrorism* adalah pemerasan, keinginan untuk dihancurkan,

berbagai jenis eksploitasi dan balas dendam. Dan tindakan paling umum yang dilakukan atau diancam oleh teroris adalah penghancuran fisik, penghancuran data dan informasi penting, serangan terhadap system komputer yang sangat penting, serbuan illegal ke dalam sistem komputer dari kepentingan publik dan penolakan akses sistem, layanan, dan data penting (Vilic, 2017:70).

2.3.4 Tindak Pidana Transnasional Terorganisir

2.3.4.1 Definisi Tindak Pidana Transnasional Terorganisir

Tindak pidana transnasional adalah tindak kriminal atau transaksi kriminal yang melintasi batas- batas nasional sehingga melanggar hukum lebih dari satu negara (Natarajan, 2015:xiii). Kejahatan transnasional tidak serta- merta didukung oleh faktor- factor seperti pasar bebas dunia yang terbuka luas atau dikarenakan lemahnya penegakan hukum, namun juga didukung oleh wilayah geografis yang strategis (Widyawati, 2018: 305). Sedangkan istilah terorganisir atau melibatkan organisasi kriminal memiliki arti bahwa pelaku tindak pidana haruslah grup terorganisasi yang terdiri lebih dari beberapa orang, yang terbentuk, beraksi secara bersama guna mendapat keuntungan secara finansial atau materi lainnya (Effendi, 2014:128).

2.3.4.2 Karakteristik Tindak Pidana Transnasional Terorganisir

Banyaknya perbedaan mengenai pendefinisian tindak pidana transnasional terorganisir, para ahli pun menyimpulkan beberapa karaketer yang dapat menjadi penghantar untuk mengidentifikasi tindak pidana transnasional terorganisir, karakteristik tersebut adalah sebagai berikut:

a. Pelaku: mereka adalah orang atau kelompok terorganisir yang melintasi batas- batas negara (secara fisik atau secara virtual- dengan menggunakan teknologi canggih dalam bidang informatika dan komunikasi sambil mengembangkan kegiatan mereka.
b. Objek kejahatan terorganisir, diwakili oleh: “barang haram (diproduksi atau dari bidang jasa), barang- barang tersembunyi atau barang- barang obyek penyelundupan ke luar negeri, barang lisensi yang dibeli dari suatu negara dengan melanggar batasan mengenai ekspornya, barang lisensi yang diimpor dari suatu negara dengan melanggar batasan mengenai impor atau embargo internasional.
c. Subjek kejahatan terorganisir: terdiri dari orang asing yang melakukan tindakan illegal di wilayah negara lain.
d. Motif kejahatan terorganisir: yaitu untuk mendapatkan keuntungan dari kegiatan terlarang.
e. Sinyal digital: merujuk pada pengiriman pesan elektronik yang bertujuan menyerang atau menghancurkan system informatika atau merampok lembaga keuangan.

2.3.4.3 Ciri- Ciri Tindak Pidana Transnasional Terorganisir

Menurut karakteristik diatas, kejahatan transnasional terorganisir memiliki tiga ciri berbeda yang membedakan dengan kejahatan berdimensi nasional, yaitu:

(1) Beroprasi pada tingkat regional atau global;

(2) Telah menciptakan koneksi lintas batas yang diperluas;

(3) Memiliki kapasitas untuk menantang otoritas nasional dan internasional. (Stoica, 2016: 14).

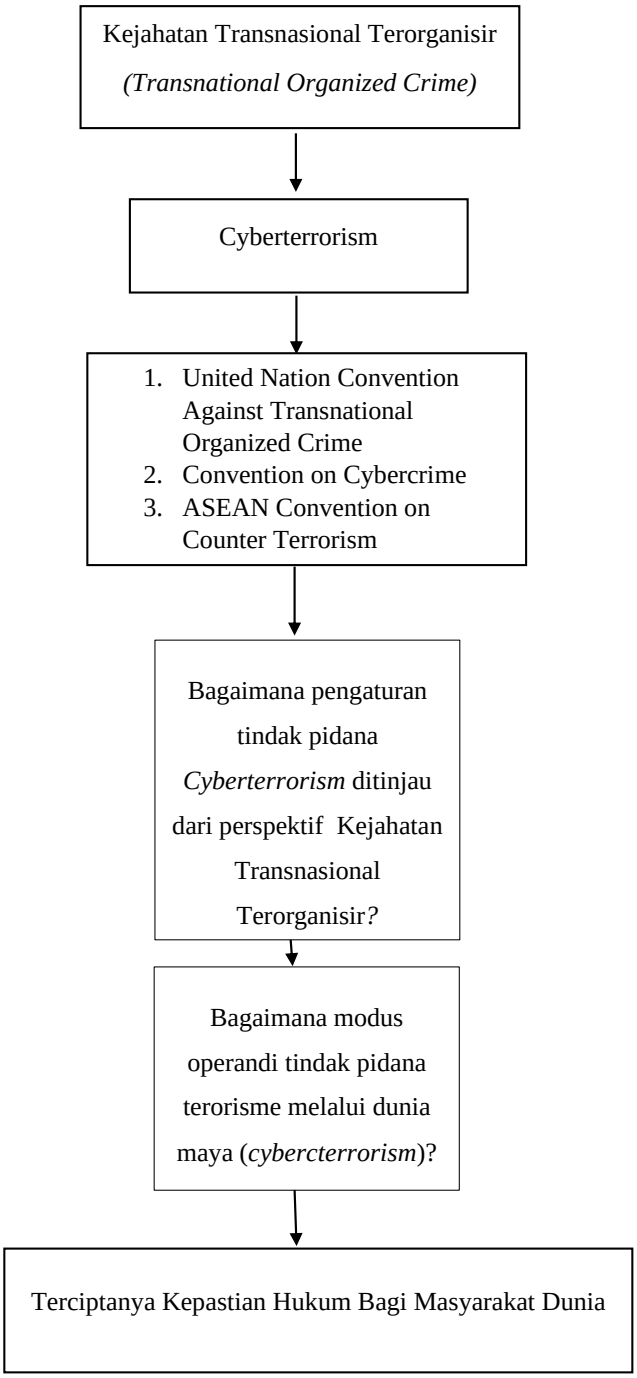
Selain karakteristik dan ciri spesifik yang harus dimiliki oleh sebuah tindak pidana agar dapat dikategorikan sebagai kejahatan transnasional terorganisir, menurut *United Nations Convention Against Transnasional Organized Crime* (UNTOC) syarat transnasional sebuah perbuatan adalah sebagai berikut:

1. Dilakukan di lebih dari satu negara
2. Dilakukan di satu negara tetapi bagian substantive dari persiapan, perencanaan, pengarahan dan pengawasannya dilakukan di negara lain.
3. Dilakukan di satu negara tetapi melibatkan suatu kelompok kejahatan terorganisasi yang ikut serta dalam kegiatan kejahatan di lebih dari satu negara.
4. Dilakukan di satu negara tetapi telah memberikan dampak yang cukup besar dinegara lain (Effendi, 2014:127).

2.3. Kerangka Berpikir

Uma Sekaran dalam buku *Research Methods for Business (2000)* yang dikutip J Supranto menyatakan bahwa, kerangka berpikir didefinisikan sebagai sebuah model yang berkosep tentang bagaimana sebuah teori memiliki korelasi dengan macam- macam variabel dan faktor yang teridentifikasi sebagai sebuah masalah yang besar. Dalam kerangka berpikir teori antar variable yang telah dipilih untuk diteliti akan dijelaskan secara

teoritis, khususnya mengenai hubungan antara- variabel tak bebas (*dependent*) dan variabel bebas (*independent*) (Supranto, 2003:195).



BAB V

PENUTUP

5.1. Simpulan

Berdasarkan penelitian dan pembahasan yang telah dilakukan penulis, maka dapat ditarik simpulan:

(1) *Cyber terrorism* merupakan bagian dari *Cybercrime* dan tindak pidana terrorisme. Serta mengingat sifat *borderless* dari *Cyber terrorism* maka *Cyber terrorism* dapat dikategorikan sebagai kejahatan transnasional. Berdasarkan perspektif kejahatan transnasional, terdapat dua atau lebih negara yang memiliki kewenangan yurisdiksi guna melakukan penegakan tindak pidana *Cyber terrorism*, sehingga instrument hukum yang digunakan sebagai sumber penegakan dapat bersalah dari hukum nasional suatu negara dan sumber hukum pidana internasional. Contohnya adalah Indonesia, Indonesia memiliki dua instrument hukum yang dapat digunakan sebagai sumber hukum penegakan tindak pidana *Cyber terrorism,* yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta Undang- Undang Nomor 5 Tahun 2018 tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme. Serta menurut hukum pidana internasional terdapat beberapa konvensi internasional yang dapat digunakan sebagai instrument hukum pengatur tindak pidana *Cyber terrorism*. Konvensi internasional tersebut adalah *United Nations Convention against Transnational Organized Crime*

Palermo, Italy tahun 2000; *Convention on Cybercrime* Budapest tahun 2001; dan *International Convention for the Suppression Of Terrorist Bombing* New York, Amerika Serikat tahun 1998. Unsur- unsur tindak pidana yang diatur dalam ketiga konvensi tersebut telah terbukti sesuai dengan unsur- unsur tindak pidana *Cyber terrorism*, sehingga konvensi internasional tersebut dapat menjadi instrument hukum pengatur tindak pidana *Cyber terrorism.*

(2) Teroris dalam melakukan tindak pidana *Cyber terrorism* memiliki modus operandi yang berbeda- beda. Dikarenakan internet dapat diekspoitasi dengan mudahnya membuat organisasi teroris memiliki berbagai cara untuk melakukan tindak pidana tersebut. Organisasi teroris seperti ISIS memanfaatkan internet untuk membantu mereka mewujudkan tujuannya. ISIS membuat serta memanfaatkan organisasi peretas untuk memudahkan mereka dalam melakukan tindak pidana *Cyber terrorism.* ISIS dibantu oleh *Cyber Caliphate Army (CCA); Sons Caliphate Army (SCA) Kalashnikov E-Security Team; United Cyber Caliphate; The Islamic State Hacking Division (ISHD); Islamic Cyber Army (ICA); The group Rabitat AL- Ansar; dan Tim Cyber Rox (CTR).* Berdasarkan berbagai kegiatan yang dilakukan oleh organisasi peretas tersebut dapat diketahui modus operandi yang digunakan oleh ISIS dalam melakukan tindak pidana Cyber terrorism, yaitu dengan melakukan *Cyber attack* berupa peretasan, propaganda, penipuan guna mendapatkan pendanaan, serangan *Distributed Denial of Service (DDoS)* dan serangan *Malware.*

5.2. Saran

(1) Perlu dirumuskannya definisi pasti dari tindak pidana *Cyber terrorism* dikarenakan banyaknya pendapat yang berbeda mengenai definisi tindak pidana *Cyber terrorism* membuat tindak pidana tersebut tidak dapat diidentifikasi dengan jelas unsur- unsurnya yang mengakibatkan sulitnya menemukan instrument hukum pengatur yang sesuai dengan tindak pidana *Cyber terrorism*. Juga diperlukannya instrument hukum pengaturan tindak pidana *Cyber terrorism* khusus yang secara global dapat digunakan oleh negara- negara di dunia sebagai dasar hukum penegakan tindak pidana *Cyber terrorism*. Dikarenakan perkembangan teknologi yang semakin pesat sejalan dengan tingginya angka kejahatan berbasis teknologi seperti *Cyber terrorism.* Diperlukan kepastian hukum yang nyata guna pencegahan dan penegakan hukum tindak pidana *Cyber terrorism*. Negara- negara di dunia juga sebaiknya meratifikasi berbagai macam konvensi internasional yang dapat digunakan sebagai instrument hukum pengatur tindak pidana *Cyber terrorism.*

(2) Luasanya jangkauan internet mengharuskan para penggunanya lebih berhati- hati dalam menggunakan internet. Seperti yang telah kita ketahui bahwa modus opernadi yang digunakan oleh organisasi teroris sangatlah beragam, maka diperlukan penyaringan informasi atau konten yang diakses oleh para pengguna internet. Supaya pengguna internet tidak menerima informasi atau konten yang salah sehingga tidak mudah terpengaruh oleh hal- hal yang menyesatkan dikemudian hari. Sosialisasi mengenai pengetahuan bagaiamana cara memanfaatkan internet dengan benar serta

bersosial media yang aman juga dirasa perlu untuk diberikan kepada pengguna internet. Serta diperlukanya pengetahuan hukum yang mencukupi bagi pengguna internet supaya pengguna internet tidak berani melakukan kejahatan berbasis internet, mengetahui konsekuensi terhadap segala hal yang mereka lakukan di dunia maya serta mengetahui hal- hal yang harus dilakukan jika menemukan atau mengalami kejahatan berbasis teknologi.

Daftar Pustaka

1. Buku

Akhgar, B. Staniforth, A. dan Bosco, F. 2014. *Cybercrime and Cyber terrorism Investigator;s Hand Book. Waltham*, MA: Syngress Publishing

Ali, Zainuddin. 2013. *Metode Penelitian Hukum*. Jakarta: Sinar Grafika.

Alkhouri, L. Kassirer, A. dan Nixon, A. 2016. *Hacking for ISIS*. Falshpoint Publisher

Amiruddin dan Asikin Z. 2004. *Pengantar Metode Penelitian Hukum*. Jakarta: Raja Grafindo.

Arief, Barda N. 2008. *Bunga Rampai Kebijakan Hukum Pidana.* Jakarta: Prenadamedia Grup

Ariman, Rasyid dan Raghib F. 2015. *Hukum Pidana*. Malang: Setara Pers

Atmasasmita, Romli. 1995. *Pengantar Hukum Pidana Internasional*. Bandung: Eresco.

Charvat, M. 2009. *The Virtual Battlefield: Perspectives on Cyber Warfare: Cyber terrorism: A new Dimension in Battlespace*. IOS Press

Conway, M. 2014. *Cyber terrorism.* New York: Springer Recuperado

Dayan, Rahmani. 2015. *Sistem Pemidanaan Terhadap Pelaku Tindak Pidana Terorisme Sebagai Extra Ordinary Crime Di Indonesia*. Yogyakarta: Genta Publishing.

Effendi, Tolib. 2014. *Hukum Pidana Internasional*. Surabaya: Pustaka Yustisia.

Fajar M. dan Achmad Y. 2017. *Dualisme Penelitian Hukum Normatif Empiris (4th Ed.)*. Yogyakarta: Pustaka Pelajar.

Hartono, Sunaryati. 2006. *Penelitian Hukum di Indonesia Pada Akhir Abad Ke-20 (Cet II)*. Bandung: Penerbit Alumni.

Hazeltine, B. 2003. *Field Guide to Appropiate Technology*. Brown University: Academic Press

Ibrahim, Johni. 2007. *Teori dan Metodologi Penelitian Hukum Normatif (Cet III).* Malang:Banyumedia Publishing.

Johan, Bahder. 2008. *Metode Penelitian Hukum*. Bandung: CV. Mandar Maju.

Kristanto, Vigih H. 2018. *Metode Penelitian Pedoman Penulisan Karya Ilmiah*, Yogyakarta: Deepublish.

Masyhar, Ali. 2009. *Gaya Indonesia Menghadang Terorisme, Sebuah Kriti katas Kebijakan Hukum Pidana Terhadap Tindak Pidana Terorisme di Indonesia.* Bandung: Mandar Maju.

Marzuki, Peter Mahmud. 2005. *Penelitian Hukum*. Jakarta: Kencana Prenada Media Grup. Jakarta: PT. Raja Grafindo

Maramis, Frans. 2012. *Hukum Pidana Umum dan Tertulis di Indonesia.*

Moeloeng, Lexy J. 2007. *Metodologi Penelitian Kualitatif*. Bandung: PT. Remaja Rosda Karya.

Natarajan, Mangai. 2015. *International and Transnational Crime and Justice*. New York: Cambridge University Pers.

Parthiana, I Wayan. 2006. *Hukum Pidana Internasional*. Bandung: Yrama Widya.

Prasetyo, Teguh. 2010. *Hukum Pidana.* Jakarta: PT. Raja Grafindo Persada

Soekanto, S dan Mamaudji, S. 2001. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Raja Grafindo.

Soemitro, Ronny H. 1990. *Metodologi Penelitian Hukum dan Jurimetri (Cet IV)*. Jakarta: Ghalia Indonesia.

Stroobants, S. 2018. *Expert Contributions: Cyber terrorism is the New Frontier*. Global Terrorism Index.

Sudarto. 1981. *Hukum dan Hukum Pidana*. Bandung: Alumni.

Sudarto. 2009. *Hukum Pidana I.* Semarang: Yayasan Sudarto Fakultas Hukum Undip.

Sunggono, Bambang. 2006. *Matodologi Penelitian Hukum*. Jakarta: Gramedia.

Supranto, J. 2003. *Penelitian Hukum dan Statistik*. Jakarta: Rineka Cipta.

Surayin. 2005. *Analisis Kamus Umum Bahasa Indonesia*. Bandung: Yrama.

Suseno, Sigid. 2012. *Yurisdiksi Tindak Pidana Siber*. Bandung: PT.Refika Pratama.

UNODC. 2012. The Use of Internet For Terrorist Purpose. New York: United Nations

Waluyo, Bambang. 2002. *Penelitian Hukum Dalam Praktek*. Jakarta: Sinar Grafika.

Widyawati, Anis. 2014. *Hukum Pidana Internasional.* Jakarta: Sinar Grafika

2. Jurnal

Al-Rawi, A. 2018. *Video games, terrorism, and ISIS's Jihad 3.0*. Terrorism and political violence journal: Vol.30 No.4. DOI: 10. 1080/09546553.2016.1207633

Astuti, S.A. 2015. *Law Enforcement of Cyber terrorism ini Indonesia.* Jurnal Rechtsidee: Vol.2 No.2. UMS Sidoarjo.

Bieda, D. Halawi, L. 2015. *Cyberspace: a venue for terrorism.* Issues in information journal:Vol 16.

Bogdanoski, M. Petreski, D. 2013. Contemporary Macedionian Defense-International Scientific Defence, Security and Peace Journal: *Cyber terrorism- global security threat.* Macedonia

Bucaj, E. 2017. *The Need for Regulation of Cyber terrorism Phenomena in Line With Principles of International Criminal Law.* Juridica: Vol 13 No 17. Galati: Universitatea Danubius.

Gordon, S dan Ford, R. *On the Definition and Classification of Cybercrime*. Journal in Compuetr and Virology.

Jarvis, L. Macdonald, S. 2015. *What is Cyber terrorism? Finding From Survey of Researchers*. Journal Terrorism and Political Violance: Vol 27 Issue 4.

Josianto, A. 2014. *Tindak Pidana Cyber terrorism Dalam Transaksi Elektronik.* Jurnal Lex Administratum: Vol.3 No.3.

Lux, L Mayer. 2018. *Defining Cyber terrorism.* Rev. chil. Dereco technol:Vol.7 No.2. Chile: Pontificia Universidad Catolica de Valparaiso

Macdonald, S., Jarvis, L. and Nouri, L., 2015. St Andrews Journal of International Relations: *State Cyber terrorism: A Contradiction in Terms? Contemporary Voices.*

Masyhar, A. 2016. *Urgensi Revisi Undang- Undang Terorisme.* Jurnal Masalah- Masalah Hukum: Jilid 45 No.1. UNDIP Semarang.

Perdana, C. 2016. Jurnal Hukum Ius Quia Iustum: *Rekonstruksi Pemidanaan Pelaku Tindak Pidana Terorisme di Indonesia.* Universitas Islam Indonesia Yogyakarta.

Sarinastiti, E.N. 2018. *Internet dan Terorisme: Menguatnya Aksi Gobal Cyber-Terroism Melalui New Media.* Jurnal Gama Societa: Vol.1 No.1. UGM Yogyakarta.

Saptoajie, S. Widyawati, A. 2016. *Digging Over The Causal Factors and Conflict Resolution for Juvenile Delicuency/ Juveline Deliquent.* South East Asia Journal of Contemporary Business, Economics and Law, Vol.10, Issue.4.

Stoica, I. 2016. *Transnational Organized Crime An International Security Perspective*. Journal of Defense Resource Management: Vol.7 Issue 2 (13). Romania: Ministry of National Defense.

Sonata, D.L. 2014. *Metode Penelitian Normatif dan Empiris: Kharakteristik Khas Dari Metode Penelitian Hukum.* Volume 8 Nomor 1. Universitas Negeri Lampung.

Tehrani, M Paradis. Manap, N Abdul. Taji, H. 2013. *Cyber terrorism challenges: "The need for a global response to a multi-jurisdictional crime.* Computer Law and Security Review: Vol 29. Malaysia: Faculty of Law UKM Bangi.

Terzi, M. 2019. Turkish Journal of TESAM Academy: E- Government and Cyber terrorism: *Conceptual Framework, Theoritical Discussions and Possible Solutions.* TESAM Academy Dergisi.

Vadza, K. 2013. *Cybercrime and its Categories.* Indian Journal of Applied Research: Vol.3 Issue.5.

Widiyanto, B. 2017. *Dampak Serangan Virtual ISIS Cyber Calipathe Terhadap Amerika Serikat.* Jurnal International & Diplomacy: Vol.2 No.2. Universitas Paramadina Jakarta.

Widyawati, A. Ridwan,R. 2018. *The Protection of Illegal Imigrants Under Indonesia National Law and International Law*. Advances in Social Science, Education and Humanity Research ICILS. Atlantis Press.

3. Artikel/ Proceeding Seminar

Arraromi, M Ayodeji. 2018. Cyber-terrorism under the Nigerian law: a new form of threat or an old threat in a new skin?. Nigeria

Brenner, W Susan. Schwerha, J Joseph. 2007. Business Law Today: "Cybercrime Havens: Challenges and Solutions". Vol. 17.

Brenner, S. 2006. Cybercrime, Cyber terrorism and Cyberwarfare. Vol 77.

Dalal, P. 2006. Cybercrime and Cyber terrorism: Preventive defense for cyberspace violations. Computer Crime Research.

Dogrul, M. Aslan, A. Celik, E. 2011. Developing an International Coopertaion on Cyber defence and Deterrence against Cyber terrorism. 3rd International Confrence on Cyber conflict. Estonia: CCD COE Publications

Giantas, D. Stergiou, D. 2018. From Terrorism to Cyber terrorism: The Case of ISIS. Greece.

Gomis, B. 2015. Demystifying 'Narcoterrorism'. Swansea University: CRC Press.

Gungormez, O. Alkanat, A. 2019. Environmental Terorrism and Arson Attacks on Forest by the PKK. Instanbul: SETA.

Heickero, R. 2008. 13th International Command and Control Research and Technology Symposium: C2 for Complex Endeavors: Terrorism Online and the Change of Modus Operandi. US: Department of Defense

Jahankhani, H. et al. 2014. Cybercrime Classification and Characteristic. Cybercrime and Cyber terrorism Investigator Handbook. USA: Elseiver.

Ndikilar, C. Limen, N. 2019. Nuclearterrorism and Cross border Security. Federal University Dutse Nigeria

Rajani M.K dan Chandio M.S. 2004. Use of Internet and Its Effect on Our Society. Session VIII No.2. Pakistan: University of Sindh.

Theohary, C.A. dan Rollins, J.W. 2015. Cyberwarfare and Cyber terrorism: In Brief. Congressional Reseach Service.

United State of Peace. 2001. Teaching Guide on International Terrorism: Definition, causes, and responses. United State.

Vatis, M. 2001. Cyber attacks During the War on Terrorism: A Predictive Analysis. Darmouth College: Institute for Security Technology Studies.

Vilic, V. 2017. Cyber terrorism on The Internet and Social Networking: A Threat to Global Security. International Scientific Confrence on Information Technology and Cata Related Research Serbia: Singidunum University.

Zerzri, M. 2017. The Threat of Cyber terrorism and Recommendations for Countermeasures. No 4. C.A. Perpective on Tunisia

4. Encyclopedia/ Article dalam Encyclopedia dan Kamus

McQuade, S.C. 2009. Encyclopedia of Cybercrime. USA: Greenwood Pers

The Concise Oxford Dictionary of Current English (8th edition). 1990. Oxford: Clarendon Press

5. Lain- Lain

Collin, B. Cyber terrorism is real- is it? Introduction in the 1980's Barry Collin. Diakses di http://www.intelligence-and-investigations.com/media/uploads/62_Cyber terrorism%20-%20Nicholas%20Bradley.pdf pada 21/10/2019.

Weimann, G. 2004. Cyber terrorism: How Real is The Threat?. United State Institute of Peace Special Report. Washington DC. Diakses di https://www.usip.org/sites/default/files/sr119.pdf pada 21/10/2019.

Whiting, A. Macdonald, S. Jarvis, L. Cyber terrorism: Understandings, Debates and Representations 2018. Diakses di https://www.cambridge.org pada 14/ 01/ 2019