

**TINJAUAN YURIDIS TERHADAP PELAKU *CYBER
TERRORISM* MENURUT UNDANG-UNDANG NOMOR
15 TAHUN 2003 TENTANG PEMBERANTASAN
TINDAK PIDANA TERORISME**

SKRIPSI

**Diajukan Guna Memenuhi Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Hukum
Program Studi Ilmu Hukum**

Oleh:

**M. HABIBIE GINTING
1206200441**



**FAKULTAS HUKUM
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2016**



Ilmu, Cerdas dan Berprestasi

MAJELIS PENDIDIKAN TINGGI, PENELITIAN & PENGEMBANGAN
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM

Jalan Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6623301 Fax. (061) 6625474
Website : <http://www.umsu.ac.id> E-mail : rektor@umsu.ac.id
Bankir : Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

BERITA ACARA
UJIAN MEMPERTAHANKAN SKRIPSI SARJANA
BAGI MAHASISWA PROGRAM STRATA I

Panitia Ujian Sarjana Strata I Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dalam sidangnya yang diselenggarakan pada hari Rabu, tanggal 26 Oktober 2016, Jam 12.00 WIB sampai dengan selesai, setelah mendengar, melihat, memperhatikan menimbang:

MENETAPKAN

NAMA : M. HABIBIE GINTING
NPM : 1206200441
PRODI/BAGIAN : ILMU HUKUM/HUKUM PIDANA
**JUDUL SKRIPSI : TINJAUAN YURIDIS TERHADAP PELAKU CYBER
TERRORISM MENURUT UNDANG-UNDANG NOMOR
15 TAHUN 2003 TENTANG PEMBERANTASAN
TINDAK PIDANA TERORISME**

Dinyatakan : (B) Lulus Yudisium dengan predikat Baik
() Lulus Bersyarat, memperbaiki/Ujian Ulang
() Tidak Lulus

Setelah lulus, dinyatakan berhak dan berwenang mendapatkan gelar Sarjana Hukum (SH) dalam BAGIAN HUKUM PIDANA.

PANITIA UJIAN

Ketua

IDA HANIFAH, S.H., M.H
NIDN: 0003036001

Sekretaris

FAISAL, S.H., M.Hum
NIDN: 0122087502

ANGGOTA PENGUJI:

- 1. IDA NADIRAH, S.H., M.H**
- 2. M. NASIR SITOMPUL, S.H., M.H**
- 3. ASLIANI HARAHAP, S.H., M.H**
- 4. RACHMAD ABDUH, S.H., M.H**

-
-
-
-



Siagap, Cerdas dan Berprestasi

MAJELIS PENDIDIKAN TINGGI, PENELITIAN & PENGEMBANGAN
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM

Jalan Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6623301 Fax. (061) 6625474
Website : <http://www.umsu.ac.id> E-mail : rektor@umsu.ac.id
Bankir : Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

PENDAFTARAN UJIAN SKRIPSI

Pendaftaran Skripsi Sarjana Fakultas Hukum Universitas Muhammadiyah Sumatera Utara Strata I bagi:

NAMA : M. HABIBIE GINTING
NPM : 1206200441
PRODI/BAGIAN : ILMU HUKUM/HUKUM PIDANA
JUDUL SKRIPSI : TINJAUAN YURIDIS TERHADAP PELAKU *CYBER TERRORISM* MENURUT UNDANG-UNDANG NOMOR 15 TAHUN 2003 TENTANG PEMBERANTASAN TINDAK PIDANA TERORISME

PENDAFTARAN : Tanggal 22 Oktober 2016

Dengan diterimanya Skripsi ini, sesudah lulus dari Ujian Komprehensif, penulis berhak memakai gelar:

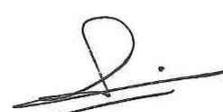
SARJANA HUKUM
BAGIAN HUKUM PIDANA

Diketahui
Dekan


IDA HANIFAH, S.H., M.H
NIDN: 0003036001

Pembimbing I

Pembimbing II


ASLIANI HARAHAP, S.H., M.H
NIDN: 0126066802


RACHMAD ABDUH, S.H., M.H
NIDN: 0004127204



Ilmu, Cerdas dan Berprestasi

MAJELIS PENDIDIKAN TINGGI, PENELITIAN & PENGEMBANGAN
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM

Jalan Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6623301 Fax. (061) 6625474

Website : <http://www.umsu.ac.id> E-mail : rektor@umsu.ac.id

Bankir : Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

LEMBAR PERSETUJUAN PEMBIMBING

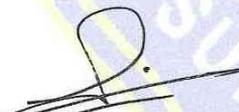
NAMA : M. HABIBIE GINTING
NPM : 1206200441
PRODI/BAGIAN : ILMU HUKUM/HUKUM PIDANA
JUDUL SKRIPSI : TINJAUAN YURIDIS TERHADAP PELAKU *CYBER
TERRORISM* MENURUT UNDANG-UNDANG NOMOR
15 TAHUN 2003 TENTANG PEMBERANTASAN
TINDAK PIDANA TERORISME

Disetujui Untuk Disampaikan Kepada
Panitia Ujian

Medan, 22 Oktober 2016

Pembimbing I

Pembimbing II


ASLIANI HARAHAP, S.H., M.H

NIDN: 0126066802


RACHMAD ABDUH, S.H., M.H

NIDN: 0004127204



Ilmu, Cerdas dan Berprestasi

MAJELIS PENDIDIKAN TINGGI, PENELITIAN & PENGEMBANGAN
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM

Jalan Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6623301 Fax. (061) 6625474
Website : <http://www.umsu.ac.id> E-mail : rektor@umsu.ac.id
Bankir : Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini:

Nama : M. Habibie Ginting
NPM : 1206200441
Program : Strata - I
Fakultas : Hukum
Program Studi : Ilmu Hukum
Bagian : Hukum Pidana
Judul : TINJAUAN YURIDIS PELAKU *CYBER TERRORISM*
MENURUT UNDANG-UNDANG NOMOR 15 TAHUN 2003
TENTANG PEMBERANTASAN TINDAK PIDANA
TERORISME

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis ini secara keseluruhan adalah hasil penelitian/karya saya sendiri, kecuali pada bagian-bagian yang dirujuk sumbernya.

Dan apabila ternyata di kemudian hari skripsi ini merupakan hasil plagiat atau merupakan karya orang lain, maka dengan ini saya menyatakan bersedia menerima sanksi akademik dari Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.

Medan, Oktober 2016

Saya yang menyatakan



M. HABIBIE GINTING

ABSTRAK
**Tinjauan Yuridis Terhadap Pelaku *Cyber Terrorism* Menurut
Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan
Tindak Pidana Terorisme.**

M. HABIBIE GINTING
NPM: 1206200441

Penelitian ini membahas salah satu kasus pidana tentang Tinjauan Yuridis Terhadap Pelaku *Cyber Terrorism* Menurut Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme. Pada dasarnya suatu kegiatan dalam melakukan tindak pidana *Cyber Terrorism* suatu kejahatan yang digambarkan sebagai suatu tindakan terorisme yang dilakukan dengan menggunakan komputer. Bentuk terorisme tersebut beralih dari terorisme yang dilakukan di dunia nyata (fisik) ke dalam bentuk terorisme melalui dunia maya (*cyber*), atau dengan kata lain *cyber terrorism* itu merupakan kejahatan terorisme dengan menggunakan ruang maya (*cyber space*) dalam melakukan kejahatannya. Untuk mencapai suatu tujuan tertentu baik untuk menyerang negara ataupun masyarakat.

Tujuan dilakukannya penelitian ini adalah untuk mengetahui pengaturan hukum pidana mengenai Tinjauan Yuridis Terhadap Pelaku *Cyber Terrorism* Menurut Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme. Untuk mengetahui faktor apa saja yang mengakibatkan maraknya *cyber terrorism*, pengaturan hukum pelaku *cyber terrorism* menurut Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme, akibat hukum pelaku *cyber terrorism* Menurut Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme. Penelitian ini merupakan penelitian hukum yuridis normatif dengan menggunakan data sekunder, dengan studi dokumentasi dan penelusuran kepustakaan.

Bedasarkan hasil penelitian dapat dipahami bahwa faktor hukum mengenai *cyber terrorism* yaitu adanya ketergantungan pada komputer, kelemahan sistem yang dapat dieksploitasi, nilai informasi yang semakin berharga, bertambahnya jumlah operator komputer, banyaknya jumlah *software* yang tersedia sehingga memudahkan kegiatan *hacking/cracking*, mengabaikan sikap waspada pada penggunaan konfigurasi keamanan jaringan. Pengaturan hukum mengenai *cyber terrorism* adalah Undang-undang Nomor 15 Tahun 2003, Pasal 155 ayat (1), 156, 157 ayat (1), 160 KUHP dan Pasal 28 Ayat (2) j.o Pasal 45 Ayat (2) Undang-undang Nomor 11 Tahun 2008. Adapun kendala pelaksanaan Undang-undang Nomor 15 Tahun 2003 yaitu intern meliputi adanya aturan pasal yang lemah seperti pada Pasal 26 dan kendala ekstern yaitu yang berasal dari luar undang-undang itu sendiri meliputi baik dari kurangnya sarana yang memadai bagi polisi dalam menjalankan tugasnya, keterbatasan pengetahuan/ tenaga ahli, dan kurangnya kepercayaan masyarakat terhadap Polisi.

Kata Kunci: Pelaku, Tindak Pidana, *Cyber Terrorism*

KATA PENGANTAR



Assalamu'alaikumWr.Wb

Segala puji dan syukur kehadiran Allah SWT, serta shalawat dan salam kepada Nabi Muhammad SAW, keluarga, sahabatnya hingga akhir zaman semoga kita mendapat syafaatnya, sehingga penulis dapat menyelesaikan Skripsi ini guna memenuhi salah satu syarat untuk memperoleh gelar Sarjana Hukum (SH) dalam ilmu Hukum pada jurusan Hukum Pidana Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.

Syukur alhamdulillah dengan rahmat dan ridho-Nya disertai dengan usaha-usaha dan kemampuan yang ada, Skripsi dengan judul **“Tinjauan Yuridis Terhadap Pelaku Cyber Terrorism Menurut Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme”**, dapat diselesaikan tepat pada waktu yang diinginkan.

Disadari sepenuhnya keterbatasan yang dimiliki, kekurangan dan kekhilafan yang ada pada diri penulis. Meskipun telah berusaha untuk memberikan yang terbaik namun masih banyak kekurangan-kekurangan atau kesalahan-kesalahan. Maka untuk itu dengan senang hati menerima saran-saran dan kritik yang sehat dari semua pihak yang sifatnya membangun guna menunjang kesempurnaan Skripsi ini.

Pada kesempatan ini, ingin disampaikan ucapan terima kasih dan penghargaan yang setinggi-tingginya kepada semua pihak yang telah banyak memberi bantuan dalam menyelesaikan Skripsi, terutama sekali kepada :

Teristimewa diucapkan terima kasih yang tak terhingga kepada Ayahanda **H. Mahmuddin Ginting**, dan Ibunda **Hj. Saniah Br. Surbakti** yang telah memberikan bantuan materil, moril, pengorbanan, bimbingan dan do'a, kasih sayang serta telah bersusah payah membesarkan penulis semoga ALLAH SWT melimpahkan rahmat dan karunia kepada ayahanda dan ibunda.

Kepada Bapak **Dr. Agussani MAP.**, selaku Rektor Universitas Muhammadiyah Sumatera Utara. Ibu **Ida Hanifah, SH., M.H.**, selaku Dekan Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Bapak **Faisal, SH., M.Hum**, dan bapak **Zainuddin, SH., M.H.**, selaku wakil Dekan I dan wakil Dekan III Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Bapak **Guntur Rambe, SH., M.H.** selaku kepala jurusan Hukum Pidana. Bapak dan Ibu Dosen Fakultas Hukum Universitas Muhammadiyah Sumatera Utara yang selalu meluangkan waktu dan menyalurkan ilmunya kepada penulis.

Ibu **Asliani, SH., M.H.**, selaku pembimbing I Skripsi penulis dengan ikhlas membantu dan mengajari dari penyusunan skripsi ini tanpa bapak skripsi ini tidak akan selesai. Bapak **Rachmad Abduh, SH., M.H.**, selaku pembimbing II Skripsi penulis dengan ikhlas membantu dan mengajari dari penyusunan skripsi ini tanpa ibu skripsi ini tidak akan selesai. Kepada Staf Pengajar dan pegawai yang tidak bisa penulis sebutkan satu persatu yang ada di Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Kepada kakanda dan adinda **Dewi Puspa Sari**

Ginting, Amd., Iskandar Muda Ginting, SE., Muhammad Husni Thamrin Ginting, SE., Mahendra Syahputra Ginting, SE., Evi Destika Sari Ginting, S.Psi., dan Almh. Fauziah Nur Ginting yang selalu mensupport penulis dalam pembuatan skripsi ini. Spesial buat **Hilda Novita Sari, S.Kom.** yang selalu mensupport penulis, memberikan nasihat, dan arahan dalam pembuatan Skripsi ini, dan sama-sama berjuang untuk menyelesaikan kuliah. Kepada sahabat-sahabatku **Anugrah Septiranta Sitepu, Tuffail M. Lubis, Heri Syahputra Sinaga, Doli Aulia Harahap, Kurnia Sentana, Adyatma Ramadhan, M. Aulia Putra RN Hrp, dan M. Ali Hanafiah** yang selalu memberikan semangat dan selalu ada saat penulis dalam keadaan suka dan duka. Kepada seluruh sahabat-sahabat Fakultas Hukum angkatan 2012, terkhusus anak Pidana B-1 (Pagi) dan G-1 (Pagi) yang tidak dapat disebutkan satu persatu yang sama-sama saling berjuang dan saling meberikan semangat untuk menyelesaikan Skripsi ini.

Penulis menyadari bahwa isi Skripsi ini masih jauh dari kesempurnaan yang diharapkan oleh karena itu dengan kerendahan hati penulis mohon kritik dan saran yang sifatnya membangun dan guna melengkapi kesempurnaan Skripsi ini, yang kelak dapat berguna untuk semua pihak.

Wassalam,
Medan, September 2016

Penulis,

M. HABIBIE GINTING
NPM : 1206200441

DAFTAR ISI

	Halaman
PERNYATAAN KEASLIAN.....	i
ABSTRAK.....	ii
KATA PENGANTAR.....	iii
DAFTAR ISI.....	vi
BAB I : PENDAHULUAN.....	1
A. Latar Belakang.....	1
1. Rumusan Masalah.....	9
2. Faedah Penelitian.....	9
B. Tujuan Penelitian.....	10
C. Metode Penelitian.....	11
1. Jenis Penelitian.....	11
2. Sifat Penelitian.....	12
3. Sumber Data.....	12
4. Alat Pengumpul Data.....	13
5. Analisis Data.....	14
D. Definisi Operasional.....	15
BAB II : TINJAUAN PUSTAKA.....	16
A. Pelaku.....	16
B. <i>Cyber Terrorism</i>	22
C. Tindak Pidana.....	38

BAB III : HASIL PENELITIAN DAN PEMBAHASAN.....	47
A. Pengaturan Hukum Terhadap Pelaku <i>Cyber Terrorism</i> Menurut Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme.....	47
B. Faktor Penyebab Marak Terjadinya <i>Cyber Terrorism</i>	58
C. Kendala Dalam Pelaksanaan Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme.....	65
BAB IV : KESIMPULAN DAN SARAN.....	70
A. Kesimpulan	70
B. Saran	71

DAFTAR PUSTAKA

LAMPIRAN

BAB I

PENDAHULUAN

A. Latar Belakang

Terorisme kini berkembang lebih cepat seiring dengan cepatnya perkembangan teknologi, hingga sistem perkembangan gerakan *masif* dalam kejahatan pidana terorisme bukan lagi pada bentuk konsep konvensional dalam sebaran kebencian pada pemerintahan yang berdaulat saja, tapi banyak mencederai dan merusak kehidupan kemanusiaan dalam konsep pemikiran radikalisme dan berkembang menjadi radikalisasi. Perkembangan teknologi terjadi dengan pesat dan tanpa batas (*borderless*) membawa dampak pada setiap orang dalam proses interaksi kehidupannya. Perkembangan teknologi tersebut terkait dengan penggunaan teknologi informasi yang bergerak menggunakan sistem *internet connection network*.

Aspek perkembangan terhadap kemanfaatan internet itu memasuki ruang lini kehidupan masyarakat tanpa mengenal strata yang hidup dalam tatanan bentuk kehidupan masyarakat yang telah lama berjalan dengan keteraturan norma dan nilainya. Konsekuensi terjadinya perkembangan teknologi dengan dunia internet itu menuai dampak negatif dan positif dalam proses pergaulan internasional dengan menggunakan desain teknologi internet di dalam penggunaan ruang maya.

Pada perkembangannya, dengan ditemukannya komputer sebagai produk ilmu pengetahuan dan teknologi, terjadinya konvergensi antara teknologi

telekomunikasi, media, dan komputer. Konvergensi antara teknologi telekomunikasi, media dan komputer telah menghasilkan sarana baru yang disebut internet. Internet telah memberikan sesuatu yang sama sekali baru untuk manusia. Berkembangnya ilmu pengetahuan dan teknologi telah menjadikan pembangunan menjadi lebih maju dan pertumbuhannya lebih cepat. Penemuan ilmiah pada bidang teknologi yang ada sekarang mempercepat perkembangan dari fase ke fase berikutnya.¹

Dampak positif yang ada terjadi dalam ruang kehidupan nyata adalah mempermudah percepatan komunikasi dan informasi yang ada dalam kelanjutan capaian pada sasaran yang dituju. Kehidupan sosial begitu dinamis dalam pemerataan informasi dengan berbagai peristiwa yang terjadi diberbagai belahan dunia dapat diketahui dalam hitungan detik. Namun sebaliknya berbagai peristiwa tadi yang terjadi diantaranya adalah peristiwa akibat dari perilaku dan perbuatan hukum yang menyimpang dari kelaziman manusia, dengan menggunakan media sosial sebagai alat untuk menggerakkan maksud dan mencapai tujuan negatifnya, misal gerakan masif menyebarkan ideologi dari kelompok radikalisis yang menginginkan orang percaya bahwa gerakan yang dilakukannya adalah benar, setelah itu melakukan tindak lanjut dengan memberikan pandangan bahwa pemerintahan yang sah dan berdaulat perlu dihancurkan dengan suatu gerakan tindakan nyata di luar ruang *cyber* dengan memberikan ancaman tekanan yang menimbulkan ketakutan pada semua orang atau yang dikenal dengan teror.

¹ Abdul Manan. 2006. *Aspek-aspek Pengubah Hukum*. Jakarta: Kencana, halaman 171.

Kondisi tersebut yang terjadi dalam era globalisasi yang mulai hadir di Abad ke-20 tepatnya saat terjadi revolusi elektronika yang memudahkan seluruh transaksi dan interaksi kehidupan manusia. Akhirnya dunia dapat menyatu dan saling tahu dan terbuka serta saling bergantung satu sama lain. Di dalam situasi itu pergerakan kemajuan teknologi itu melahirkan penggabungan komputer dengan telekomunikasi yang menghadirkan fenomena teknologi yang sangat mengagumkan yaitu mengubah konfigurasi desain komunikasi dari konvensional ke sistem digital. Dalam hal ini terjadi 3 (tiga) proses hingga mencapai dunia virtual yang menjadi nyata. dimensi pertama adalah kenyataan keras pada kehidupan empiris biasa disebut (*hard reality*), dimensi kedua merupakan kenyataan dalam keadaan simbolik dan nilai-nilai yang dibentuk (dipadankan dengan sebutan *soft reality*), maka dengan dimensi ketiga dikenal kenyataan maya (*virtual reality*) yang melahirkan suatu format masyarakat lainnya.

Masuknya ilmu pengetahuan dan teknologi sekarang ini berbanding lurus dengan cepatnya arus informasi keseluruh dunia. Apa yang terjadi saat ini dari bumi sebelah utara akan cepat tersebar dan akan cepat diketahui dalam hitungan menit dari belahan bumi yang lainnya. Sehingga majunya teknologi mengakibatkan lebih dekatnya jangkauan dunia karena jarak dan waktu tidak lagi menjadi hambatan.²

Terkait dengan hal tersebut di atas dengan kemajuan teknologi yang tertuju pada kemajuan telekomunikasi, multimedia dan teknologi informasi (telematika) yang akhirnya memberikan dampak perubahan pada tatanan

² *Ibid.*, halaman 171-172.

organisasi dan hubungan masyarakat, karena tidak dapat dihindari fleksibilitas dan kemampuan telematika dengan cepat memasuki berbagai aspek kehidupan manusia. Kemajuan teknologi dengan penemuan internet merupakan satu penyebab terjadinya perubahan sosial dan penyebab terjadinya pertentangan dalam masyarakat diantaranya adalah revolusi dalam ruang masyarakat, dalam kehidupan manusia banyak alasan yang dapat dikemukakan sebagai penyebab timbulnya suatu perubahan di dalam masyarakat, tetapi perubahan dalam penerapan hasil-hasil teknologi modern dewasa ini banyak disebut-sebut sebagai salah satu sebab bagi terjadinya perubahan sosial.

Sejalan dengan hal di atas, kemajuan di bidang teknologi akan berjalan dengan munculnya perubahan-perubahan di bidang kemasyarakatan. Perubahan-perubahan itu dapat mengenai nilai sosial, kaidah-kaidah sosial, pola-pola perikelakuan, organisasi dan susunan lembaga kemasyarakatan. Kemajuan teknologi membawa tuntutan tersendiri dalam kehidupan masyarakat dalam ketentuan kebutuhan masyarakat, pemerintah dan regulasi yang mengatur kehidupan dalam ruang terbuka atas penggunaan teknologi informasi yang berkembang dan membawa dampak perubahan perilaku budaya hukum dengan sebuah pertanggungjawaban dalam pola hukum baru.

Kenyataan itu adalah dengan penegakan hukum terhadap banyaknya tindak kejahatan yang kini mulai bergerak dan dilakukan dari ruang *cyber*. Pengaruh dari penggunaan media internet dan dengan pola komunikasi yang semakin aktif di berbagai bentuk media sosial semakin membuka kreatifitas pola perilaku budaya hukum yang menyimpang dari bentuk pola kejahatan

konvensional. Beberapa jenis tindak pidana semakin mudah dilakukan, bahkan yang terjadi semakin banyak tindak pidana dilakukan atas nama kebebasan tanpa batas di ruang maya tersebut.

Sebut saja semakin tinggi angka kejahatan pencemaran nama baik, pornografi, prostitusi, pembobolan rekening, perusakan jaringan *cyber (hacking)*, sampai dengan penanaman ideologi melalui tindakan komunikasi dengan *hate speech* terhadap pemerintahan berdaulat, bahkan kejahatan terorisme dari ruang maya itu terus berkembang dengan pola yang beragam. Kejahatan *cyber* belakangan sangat dikenal dalam bentuk kejahatan model baru dewasa ini. Kejahatan *cyber* terkait dengan perubahan perilaku budaya hukum yang menyentuh setiap orang dalam interaksi sosial akibat dari pesatnya penggunaan teknologi informasi.

Akibat dari penggunaan teknologi informasi dengan perangkat bernama komputer itu melahirkan gaya hidup yang berbeda dalam kenyataan yang sebenarnya. Perilaku budaya hukum dalam setiap orang di dunia maya berbeda hingga melahirkan istilah-istilah baru dalam pola kehidupan di dunia dunia maya.

Dampak secara umum keberadaan teknologi informasi memberikan pengaruh terhadap terjadinya perubahan dari akibat kemajuan teknologi informasi yang berkembang yaitu terjadinya masalah-masalah sosial. Kondisi itu dikarenakan masyarakat yang belum siap menerima perubahan secara cepat akan dampak dari kehadiran komputer atas asas kemanfaatan yang begitu besar baik positif maupun negatif. Perubahan yang terjadi bukan saja dalam bentuk pola berpikir tetapi juga telah mengurai nilai-nilai masyarakat lebih luas lagi dari nilai-

nilai baku dalam tatanan masyarakat konvensional, dan perubahan itu melahirkan masyarakat dunia maya secara virtual menjadi nyata. perubahan yang terjadi juga memberikan dampak buruk pada pola kejahatan gaya baru yang lebih dikenal di dalam tindak pidana sebagai kejahatan di ruang maya.

Perilaku budaya hukum masyarakat kini telah bergeser, dari mampu menghargai orang lain, dan mentaati nilai, norma dan kaidah hukum yang berlaku pada kelaziman di dalam masyarakat, kini atas nama kebebasan hak asasi manusia, seseorang dapat berlaku sekehendak hati dan atas kepentingan yang melekat dalam dirinya.

Kemanfaatan media (*the convergence media*) membawa perubahan pada perilaku dalam penggunaan teknologi informasi, ketika setiap orang tidak mampu memahami hakikat perubahan dalam bidang teknologi informasi itu. Akibat pengaruh penggunaan media internet dalam kehidupan masyarakat dewasa ini yang paling nyata tidak hanya memperoleh kemudahan dalam segala urusan secara legal, tetapi terjadi juga munculnya jenis tindak pidana yang semakin banyak dilakukan dengan beragam modus operandi. Hal itu berkaitan dengan kemanfaatan teknologi yang digunakan oleh para pelaku kejahatan di ruang dunia maya (*cyberspace*) dengan istilah *cybercrime*.

Pada dasarnya *cyber crime* meliputi semua tindak pidana yang berkenaan dengan informasi, sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi itu kepada pihak lainnya (*transmitter/originator to recipient*). Ada beberapa kategori tindak pidana yang masuk dalam *cyber crime* yang dipandang merupakan *extra*

ordinary crime oleh karena bentuk kejahatannya yang masuk pada unsur kejahatan yang terorganisir dan melewati batas negara yaitu *cyber terrorism*.

Aksi terorisme yang marak belakangan ini ditenggarai merupakan hasil giat masif dari ruang *cyber*. Kejahatan berkaitan dengan ideologi dan pencucian otak (*brain wash*) mengenai paham negara dan perekrutannya dengan melakukan komunikasi aktif menggunakan alat teknologi, menjadi kegiatan utama yang digerakan kepentingan kelompok radikalisisasi untuk melakukan aksinya. Contoh nyata yang dapat kita lihat saat ini adalah organisasi Radikal IS atau yang lebih dikenal dengan ISIS (*Islamic State of Iraq and Syam/Syria*) menggunakan jejaring media sosial untuk merekrut anggota baru dan terus secara kuat mempublikasikan keberadaan kelompoknya sebagai kekuatan negara baru yang akan memimpin kekhalifahan di muka bumi dan dengan berbagai cara melakukan aksi teror melalui dunia maya.

Indonesia sebagai negara hukum berupaya membuat regulasi dalam penanganan kejahatan teknologi informasi khususnya dalam pengelolaan informasi dan transaksi elektronik beserta infrastruktur dan pengaturannya. Undang-Undang Informasi dan Transaksi Elektronik diharapkan dapat mengatasi berbagai kejahatan *cyber*, dan dikuatkan dengan ketentuan Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme. Perbuatan pidana terorisme dunia maya masuk dalam kategori kejahatan lintas batas negara yang terorganisir dan telah ditetapkan sebagai kejahatan luar biasa. Kejahatan ini menjadi ancaman serius bagi negara-negara di dunia. Menanggulangi atau biasa disebut penanganan adalah proses, cara, satu atau

serangkaian proses pekerjaan. Penanggulangan tindak kejahatan internet (*cyber crime*) terdapat pada kepolisian sebagai pembuat kebijakan, penyedia fasilitas pelayanan, dan sebagai pengawas dibidang Informasi dan Transaksi elektronik kota Medan. Dalam bukunya, Prof. Barda Nawawi Arief mengungkapkan beberapa upaya penanggulangan *cyber crime* yaitu:³

1. *Cyber crime* harus dikriminalisasikan.
2. Diperlukan sarana penal.
3. Diperlukan kerjasama antara pemerintah dan industri terhadap tujuan umum pencegahan dan penanggulangan kejahatan komputer agar internet menjadi sarana yang aman.
4. Diperlukan kerja sama internasional untuk menelusuri/ mencari penjahat di internet.

Hal ini diperlukan ketegasan sikap Pemerintah untuk menegakkan hukum dunia maya terhadap kebebasan yang berkembang di dalam media sosial. Perkembangan yang tak terukur itu di negara Indonesia diperlukan batasan dengan melakukan pertanggungjawaban hukum atas perilaku hukum yang menyimpang terhadap penggunaan alat teknologi. Upaya penegakan hukum yang tegas sebagai sikap yang jelas untuk menghentikan giat terorisme yang bergerak masif, dengan memberlakukan ketentuan Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Terorisme secara efektif.

³ Barda Nawawi Arief, 2007. *Tindak pidana mayantara: perkembangan kajian cyber crime di Indonesia*. Jakarta: Raja Grafindo Persada, halaman 7.

Berdasarkan uraian di atas, maka penulis tertarik dan terdorong untuk membahas dan mengangkat judul: **Tinjauan Yuridis Terhadap Pelaku *Cyber Terrorism* Menurut Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme.**

1. Rumusan Masalah

Perumusan masalah adalah langkah untuk mengidentifikasi persoalan yang diteliti secara jelas, biasanya berisi pertanyaan-pertanyaan kritis, sistematis dan representatif untuk mencari jawaban dari persoalan yang ingin dipecahkan. Arti penting perumusan masalah adalah sebagai pedoman bagi tujuan dan manfaat penelitian dalam rangka mencapai kualitas penelitian yang optimal. Berdasarkan hal tersebut, maka adapun rumusan masalah dari penelitian ini antara lain:

- a. Bagaimana pengaturan hukum pelaku *cyber terrorism* menurut Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme?
- b. Apa saja faktor yang mempengaruhi marak terjadinya *cyber terrorism*?
- c. Bagaimana kendala dalam pelaksanaan Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme?

2. Faedah Penelitian

Penelitian ini menjadi suatu harapan dan tujuan dari hasil-hasil penelitian ini yaitu agar dapat memberikan manfaat bagi semua pihak antara lain:

- a. Secara Teoritis

Penelitian ini berfaedah untuk menambah ilmu pengetahuan di bidang hukum khususnya mengenai pemberantasan tindak pidana terorisme melalui dunia maya. Sehingga pengetahuan tentang hukum dan dasar-dasarnya dapat diketahui dan diterapkan di masyarakat, jadi segala jenis pelanggaran, pengaturan tentang pemenuhan hak pendidikan ataupun tindak pidana terkait dalam hal tersebut dapat dikurangi. Bukan hanya seorang pakar hukum yang harus memberikan atau bahkan memperjuangkan hukum di negara ini, tetapi turut sertanya masyarakat juga dapat memberikan kemajuan di negara ini. Pengetahuan hukum secara hukum dapat ditegakkan dan diterapkan di masyarakat karena itu menjadi syarat dari kemajuan, keadilan dan ketentraman negara ini.

b. Secara Praktis

Penelitian ini dapat memberikan faedah sebagai bahan acuan dalam hukum pidana dan dapat dijadikan alat penyebarluasan informasi kepada masyarakat. Serta dapat memberikan faedah untuk masyarakat dan orang-orang untuk mengetahui bagaimana Tinjauan Yuridis Terhadap Pelaku *Cyber Terrorism* Menurut Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme.

B. Tujuan Penelitian

1. Untuk mengetahui pengaturan hukum pelaku *cyber terrorism* menurut Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme

2. Untuk mengetahui apa saja faktor yang mempengaruhi marak terjadinya *cyber terrorism*,
3. Untuk mengetahui kendala dalam pelaksanaan Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme.

C. Metode Penelitian

Metode penelitian merupakan suatu faktor permasalahan yang akan dibahas, dimana metode penelitian merupakan cara utama yang bertujuan untuk mencapai tingkat penelitian ilmiah. Dalam hal ini penelitian hukum dilakukan untuk mencari pemecahan atas isu hukum yang timbul, yaitu memberikan preskripsi mengenai apa yang seyogyanya atas isu yang diajukan.⁴ Sesuai dengan rumusan permasalahan dan tujuan penelitian maka metode penelitian yang dilakukan meliputi:

1. Jenis Penelitian

Dalam penelitian ini menggunakan penelitian hukum yang bersifat normatif, dengan pendekatan penelitian terhadap sistematika hukum. Nama lain dari penelitian hukum normatif ini adalah penelitian hukum doktriner, juga disebut sebagai penelitian perpustakaan atau studi dokumen. Disebut penelitian hukum doktriner karena penelitian ini dilakukan atau ditujukan hanya pada peraturan-peraturan yang tertulis atau bahan-bahan hukum yang lain. Sedang disebut sebagai penelitian perpustakaan ataupun studi dokumen disebabkan penelitian ini lebih banyak dilakukan terhadap data yang bersifat sekunder yang

⁴ Dyah Ochtorina Susanti dan A'an Efendi. 2014. *Penelitian Hukum (Legal Research)*. Jakarta: Sinar Grafika, halaman 1.

ada di perpustakaan.⁵ Sedangkan penelitian terhadap sistematika hukum dapat dilakukan pada peraturan Perundang-undangan tertentu atau hukum tertulis.

2. Sifat Penelitian

Sifat penelitian yang dipergunakan dalam penulisan dalam menyelesaikan skripsi ini adalah bersifat deskriptif analisis. Yang mana deskriptif analisis adalah dipergunakan untuk menggambarkan berbagai gejala dan fakta yang terdapat dalam kehidupan sosial secara mendalam.⁶ Untuk mengambil kesimpulan-kesimpulan yang berlaku secara umum sehingga mengarah pada penelitian hukum yuridis normatif yaitu suatu penelitian yang didasarkan kepada peraturan Perundang-undangan yang berlaku serta bahan-bahan hukum lainnya yang berhubungan dengan Tinjauan Yuridis Terhadap Pelaku *Cyber Terrorism* Menurut Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme.

3. Sumber Data

Sumber data yang digunakan dalam penelitian ini adalah data sekunder, yaitu dari buku-buku yang secara langsung atau tidak langsung berkaitan dengan prinsip-prinsip dari peraturan yang berkaitan dengan penelitian yang diteliti.⁷ melalui penelusuran data yang diperoleh dari studi kepustakaan atau studi literatur yang terdiri atas:

⁵ Ali Murthado dan Mustafa Kamal Rokan. 2012. *Metodologi Penelitian Hukum Suatu Pemikiran dan Penerapan*. Medan: Wal Ashri Publishing, halaman 28.

⁶ Beni Ahmad Saebani. 2009. *Metode Penelitian Hukum*. Bandung: Pustaka Setia, halaman 57.

⁷ *Ibid.*, halaman 158.

- a. Bahan hukum primer, yaitu berupa bahan hukum yang meliputi peraturan Perundang-undangan yang berhubungan dengan objek penelitian yang meliputi:
- 1) Undang-undang Dasar Negara Republik Indonesia Tahun 1945
 - 2) Undang-undang Nomor 1 Tahun 1946 Tentang Peraturan Hukum Pidana
 - 3) Undang-undang Nomor 8 Tahun 1981 Tentang Peraturan Hukum Acara Pidana
 - 4) Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme
 - 5) Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
- b. Bahan hukum sekunder, yaitu berupa bahan-bahan hukum yang bersifat pelengkap bagi bahan hukum primer. Bahan hukum sekunder dalam penelitian ini berupa buku-buku, jurnal-jurnal dan karya ilmiah yang terkait dengan objek penelitian dan buku-buku yang relevan dengan materi yang diteliti.
- c. Bahan hukum tersier, yaitu berupa bahan hukum yang memberikan penjelasan mengenai bahan hukum sekunder yang relevan dengan materi yang diteliti seperti, Kamus Besar Bahasa Indonesia (KBBI), Ensiklopedia dan bahan yang diakses dari internet.⁸

4. Alat Pengumpul Data

Alat pengumpul data yang dipergunakan dalam penelitian ini adalah:

⁸ Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. 2014. *Pedoman Penulisan Skripsi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara* . Medan: Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, halaman 6.

a. Studi kepustakaan (*library research*)

Studi kepustakaan (*library research*) adalah teknik pengumpulan data dengan mengadakan studi penelaah terhadap buku-buku, literature-literatur, catatan-catatan dan sebagainya. Dalam hal ini peneliti melakukan studi kepustakaan di perpustakaan Universitas Muhammadiyah Sumatera Utara dengan tujuan untuk memperoleh data yang relevan dengan masalah yang diteliti.

b. Studi dokumen

Studi dokumen merupakan langkah awal dari setiap penelitian hukum (baik normatif maupun sosiologis (empiris), karena penelitian hukum selalu bertolak dari premi normatif. Dalam hal ini penelitian membutuhkan data atau informasi dengan cara membaca surat-surat, pengumuman, pernyataan tertulis kebijakan tertentudan bahan-bahan tulisan lainnya.

5. Analisis Data

Metode penelitian data yang sesuai dengan penelitian hukum dengan cara deskriptif adalah menggunakan pendekatan kualitatif, penelitian secara kualitatif ini biasanya dilawankan dengan penelitian kuantitatif dengan alasan bahwa dalam kegiatan ini, peneliti tidak menggunakan angka dalam mengumpulkan data dan memberikan penafsiran terhadap hasilnya.⁹ Pendekatan kualitatif merupakan suatu analisis data yang mengungkapkan dan mengambil kebenaran dari kepustakaan, yaitu dengan menggabungkan antara informasi yang didapat dari Perundang-Undangan, peraturan-peraturan dan putusan pengadilan serta tulisan-tulisan ilmiah yang ada kaitannya dengan Tinjauan Yuridis Terhadap Pelaku *Cyber Terrorism*

⁹ Beni Ahmad Saebani. *Op. Cit.*, halaman 100.

Menurut Undang-Undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme untuk dianalisis secara kualitatif sehingga dapat memecahkan masalah yang diteliti, dapat menjawab permasalahan, serta mendapat kesimpulan untuk dipahami dengan baik dalam penelitian ini.

D. Definisi Operasional

1. Pelaku adalah subjek hukum baik orang ataupun badan hukum yang melakukan tindak pidana ataupun pelanggaran yang dapat menimbulkan keterkaitan dengan hukum, dan telah memenuhi unsur-unsur delik sehingga orang atau badan hukum tersebut dapat dijatuhkan sanksi atas perbuatannya. Pelaku dalam penelitian ini adalah pelaku yang melakukan tindak pidana *cyber terrorism*.
2. *Cyber terrorism* adalah Penyerangan dengan menggunakan komputer atau mengancam, mengintimidasi atau memaksa pemerintahan atau masyarakat, dengan tujuan untuk mencapai target politik, agama atau ideology.
3. Tindak pidana merupakan perilaku yang menyimpang dari hukum yang dibuat atau perbuatan yang bertentangan dengan peraturan hukum yang berlaku. Dan apabila perbuatan tersebut dilakukan akan mendapatkan sanksi pidana yang telah diatur oleh peraturan perundang-undangan.

BAB II

TINJAUAN PUSTAKA

A. Pelaku

Abdul Wahid dalam bukunya menegaskan bahwa segala penegakkan hukum selalu akan melibatkan manusia didalamnya dan dengan demikian akan melibatkan tingkah laku manusia juga. Hukum tidak bisa berdiri tegak dengan sendirinya, artinya ia tidak akan mampu mewujudkan segala janji-janji serta kehendak-kehendak yang tercantum dalam peraturan-peraturan hukum tersebut. Janji dan kehendak seperti itu, misalnya adalah untuk memberikan hak terhadap seseorang, untuk mengenalkan pidana terhadap seorang yang memenuhi persyaratan tertentu dan sebagainya.¹⁰ Dengan demikian dalam melakukan tindak pidana akan ada yang dinamakan pelaku.

Pelaku adalah orang yang melakukan tindak pidana yang bersangkutan, dalam arti orang yang dengan suatu kesengajaan atau suatu tidak kesengajaan seperti yang diisyaratkan oleh Undang-undang telah menimbulkan suatu akibat yang tidak dikehendaki oleh Undang-undang, baik itu merupakan unsur-unsur subjektif maupun unsur-unsur objektif, tanpa memandang apakah keputusan untuk melakukan tindak pidana tersebut timbul dari dirinya sendiri atau tidak karena gerakan oleh pihak ketiga.¹¹ Melihat batasan dan uraian diatas, sesuai

¹⁰ Abdul Wahid, Mohammad Labib. 2010. *Kejahatan Mayantara (cyber crime)*. Bandung: Refika Aditama, halaman 136.

¹¹ Barda Nawawi Arif, "Pengertian Pelaku", melalui <http://www.pengertianpelakudalamhukumpidana.com>, diakses Sabtu, 13 Agustus 2016, pukul 23:24 WIB.

dengan Pasal 55 Kitab Undang-Undang Hukum Pidana (KUHP) dapat dikatakan bahwa orang yang dapat dinyatakan sebagai pelaku tindak pidana dapat dikelompokkan kedalam beberapa macam antara lain :

1. Orang yang melakukan (*dader plagen*)

Orang ini ialah seorang yang sendirian telah berbuat mewujudkan segala anasir atau elemen dari peristiwa pidana. Dalam peristiwa pidana yang dilakukan dalam jabatan misalnya orang itu harus pula memenuhi elemen “status sebagai pegawai negeri”.

2. Orang yang menyuruh melakukan (*doen plagen*)

Disini sedikitnya ada dua orang yang menyuruh (*doen plagen*) dan yang disuruh (*pleger*). Jadi bukan orang itu sendiri yang melakukan peristiwa pidana, akan tetapi ia menyuruh orang lain, meskipun demikian *tochia* dipandang dan dihukum sebagai orang yang melakukan sendiri yang melakukan peristiwa pidana, akan tetapi ia menyuruh orang lain, disuruh (*pleger*) itu harus hanya merupakan suatu alat (*instrument*) saja, maksudnya ia tidak dapat dihukum karena tidak dapat dipertanggungjawabkan atas perbuatannya, misalnya dalam hal-hal sebagai berikut :

- a. Tidak dapat dipertanggungjawabkan menurut Pasal 44, Umpamanya A berniat akan membunuh B, tetapi karena tidak berani melakukan sendiri, telah menyuruh C (seorang gila) untuk melemparkan granat tangan kepada B, bila C betul-betul telah melemparkan granat itu, sehingga B mati, maka C tidak dapat dihukum karena tidak dapat dipertanggungjawabkan, sedang yang dihukum sebagai pembunuh ialah A.

- b. Telah melakukan perbuatan itu karena terpaksa oleh kekuasaan yang tidak dapat dihindarkan (*overmacht*) menurut Pasal 4, Umpamanya A berniat membakar rumah B dan dengan menodong pakai pistol menyuruh C supaya membakar rumah itu. Jika C menurut membakar rumah itu, ia tidak dapat dihukum karena dipaksa, sedangkan A meskipun tidak membakar sendiri, *toch* dihukum sebagai pembakar.
 - c. Telah melakukan perbuatan itu atas perintah jabatan yang tidak sah menurut Pasal 51, misalnya seorang Inspektur Polisi mau membalas dendam pada seorang musuhnya dengan memasukkan orang itu dalam kamar tahanan. Ia menyuruh B seorang agen Polisi dibawah perintahnya supaya menangkap dan memasukkan dalam tahanan orang tersebut dengan dikatakan bahwa orang itu tersangka mencuri. Jika B melaksanakan suruhan itu, ia tidak dapat dihukum atas merampas kemerdekaan orang karena ia menyangka bahwa perintah itu sah, sedang yang dihukum sebagai perampas kemerdekaan ialah tetap si Inspektur Polisi.
 - d. Telah melakukan perbuatan itu dengan tidak ada kesalahan sama sekali, misalnya A berniat akan mencuri sepeda yang sedang ditaroh di muka kantor Pos. Ia tidak berani menjalankan sendiri, tetapi ia dengan menunggu agak jauh minta tolong pada B untuk mengambilkan sepeda itu dengan dikatakan bahwa itu adalah miliknya. Jika B memenuhi permintaan itu, ia tidak salah mencuri, karena elemen “sengaja” tidak ada. Yang dihukum sebagai pencuri tetap A.
3. Orang yang turut melakukan (*mede plagen*)

Turut melakukan dalam arti kata “bersama-sama melakukan”. Sedikit-dikitnya harus ada dua orang, ialah orang yang melakukan (*pleger*) dan orang turut melakukan (*medepleger*) peristiwa pidana itu. Disini diminta, bahwa kedua orang itu semuanya melakukan perbuatan pelaksanaan, jadi melakukan anasir atau elemen peristiwa pidana itu. Tidak boleh misalnya hanya melakukan perbuatan persiapan saja atau perbuatan yang sifatnya hanya menolong, sebab jika demikian, maka orang yang menolong itu tidak masuk “*medepleger*” akan tetapi dihukum sebagai “membantu melakukan” (*medeplichtige*) tersebut dalam Pasal 56. Contoh : A berniat mencuri dirumah B dan mengajak C untuk bersama-sama melakukan. Kedua-duanya masuk rumah dan mengambil barang-barang, atau C yang menggali lubang “gasiran”, sedang A yang masuk dan mengambil barang-barangnya. Disini C dihukum sebagai “*medepleger*”, karena melakukan perbuatan pelaksanaan pencurian itu. Andai kata C hanya berdiri diluar untuk menjaga dan memberi isyarat kalau ada orang datang, maka C dihukum sebagai “*medeplichtige*” Pasal 56 sebab perbuatannya hanya bersifat menolong saja.

4. Orang yang dengan pemberian, salah memakai kekuasaan, memakai kekerasan dengan sengaja membujuk melakukan perbuatan itu (*uitlokker*).

Orang itu harus sengaja membujuk orang lain, sedang membujuknya harus memakai salah satu dari jalan-jalan seperti dengan pemberian, salah memakai kekuasaan dan sebagainya. Yang disebutkan dalam Pasal itu, artinya tidak boleh memakai jalan lain. Disini seperti halnya dengan “suruh melakukan” sedikit-dikitnya harus ada dua orang, ialah orang yang yang membujuk dan

yang dibujuk, hanya bedanya pada “membujuk melakukan” orang yang dibujuk itu dapat dihukum juga sebaga “*pleger*” sedang pada “suruh melakukan”, orang yang disuruh itu tidak dapat dihukum.

Pengertian pelaku yang dikutip dari beberapa pendapat para ahli hukum pidana antara lain:

1. Simons

Pelaku suatu tindak pidana itu adalah orang yang melakukan tindak pidana yang bersangkutan, dalam arti orang yang dengan suatu kesengajaan seperti yang disyaratkan oleh Undang-Undang atau telah melakukan tindakan yang terlarang atau mengalpakan tindakan yang diwajibkan oleh Undang-Undang, atau dengan perkataan lain ia adalah orang yang memenuhi semua unsur-unsur suatu delik seperti yang telah ditentukan di dalam Undang-Undang, baik itu merupakan unsur-unsur subjektif maupun unsur-unsur objektif, tanpa memandang apakah keputusan untuk melakukan tindak pidana tersebut timbul dari dirinya sendiri atau timbul karena digerakkan oleh pihak ketiga.

2. Pompe

Yang harus dipandang sebagai pelaku itu adalah semua orang yang disebutkan dalam Pasal 55 Kitab Undang-Undang Hukum Pidana (KUHP). Hal mana telah dikuatkan oleh memori penjelasan di mana telah dikatakan bahwa semua orang telah disebutkan dalam Pasal 55 Kitab Undang-Undang Hukum Pidana (KUHP) itu adalah pelaku.

3. Van Hamel

Bahwa seseorang yang dipandang sebagai seorang pelaku itu tidak boleh semata-mata didasarkan pada suatu anggapan, akan tetapi hal tersebut selalu harus dibuktikan.¹²

Kejahatan yang dilakukan seseorang akan menimbulkan suatu akibat yakni pelanggaran terhadap ketetapan hukum dan peraturan pemerintah. Akibat dari tindak pelanggaran tersebut maka pelaku kriminal akan diberikan sanksi hukum atau akibat berupa pidana atau pemidanaan. Sanksi tersebut merupakan pembalasan terhadap sipembuat.

Pemidanaan ini harus diarahkan untuk memelihara dan mempertahankan kesatuan masyarakat. Pemidanaan merupakan salah satu untuk melawan keinginan-keinginan yang oleh masyarakat tidak diperkenankan untuk diwujudkan pemidanaan terhadap pelaku tindak pidana tidak hanya membebaskan pelaku dari dosa, tetapi juga membuat pelaku benar-benar berjiwa luhur.

Kita dapat melihat contoh penentuan pelaku Menurut Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP) yang dimaksud dengan pencurian ialah “barangsiapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau denda paling banyak enam puluh rupiah.

Unsur tindak pidana pencurian Pasal 362 KUHP yaitu:

1. Unsur subjektif

Menguasai benda tersebut secara melawan hukum.

¹² P.A.F. Lamintang. 1996. *Dasar-Dasar Hukum Pidana Indonesia*. Bandung: Citra Aditya Bakti, halaman 593-595.

2. Unsur objektif

- a. Barang siapa.
- b. Mengambil atau *wegnemen* yaitu suatu perilaku yang membuat suatu benda berada dalam penguasaannya yang nyata, atau berada dibawah kekuasaannya atau didalam detensinya, terlepas dari maksudnya tentang apa yang ia inginkan dengan benda tersebut.
- c. Sesuatu benda.
- d. Yang sebagian atau seluruhnya kepunyaan orang lain.

Unsur Pasal 362 diatas dapat disimpulkan bahwa pelakunya adalah di unsur subyektif yang menguasai benda tersebut dengan cara melawan hukum.

Disimpulkan bahwa pelaku bukanlah hanya dia yang melakukan perbuatan pidana sendiri dan perbuatanya memenuhi rumusan delik dalam Undang-Undang tetapi juga mereka yang menyuruh melakukan, yang turut melakukan dan orang yang dengan bujuk rayu, perjanjian dan sebagainya menyuruh melakukan perbuatan pidana yang sesuai diatur pada Pasal 55 Kitab Undang-Undang Hukum Pidana (KUHP).

B. *Cyber Terrorism*

Merujuk Pendapat OC. Kaligis, Mardenis mengungkapkan bahwa secara etimologi, perkataan “teror” berasal dari bahasa Latin “*terrere*” yang dalam bahasa Inggris diterjemahkan dalam perkataan “*to fright*” yang dalam bahasa Indonesia yang berarti “menakutkan” atau “mengerikan”. Rumusan terrorisme secara terminologis, sampai saat ini masih menjadi perdebatan meskipun sudah

ada ahli yang merumuskan dan dirumuskan di dalam peraturan perundang-undangan.¹³

Pada dasarnya istilah “*terorisme*” merupakan sebuah konsep yang memiliki konotasi yang sangat sensitif karena terorisme menyebabkan terjadinya pembunuhan dan penyengsaraan terhadap orang-orang yang tidak berdosa. Tidak ada negara yang ingin dituduh mendukung terorisme atau menjadi tempat perlindungan bagi kelompok-kelompok terorisme. Tidak ada pula negara yang mau dituduh tindak terorisme karena menggunakan kekuatan (militer). Ada yang mengatakan seseorang bisa disebut teroris sekaligus sbagai pejuang kebebasan. Hal itu tergantung dari sisimana memandangnya.¹⁴

Berdasarkan hal tersebut terorisme dalam hal ini menggunakan jejaring sosial. Jejaring sosial adalah situs web yang memungkinkan pengguna untuk membangun koneksi dan hubungan dengan pengguna internet lainnya. Jejaring sosial dapat digunakan untuk tetap berhubungan dengan teman-teman, membuat kontak baru, dan menemukan orang-orang dengan minat dan ide yang sama. Akan tetapi data privasi yang ada di jejaring sosial seringkali digunakan oleh penyedia aplikasi untuk hal-hal yang mengandung kontroversi.¹⁵ Dalam penggunaan *cyber terrorism* membutuhkan jaringan internet atau jaringan sosial yang akan dapat menghubungkan kesumua tempat yang diinginkan dan bahakn kesumua orang yang dituju.

¹³ Mardenis. 2013. *Pemberantasan Terorisme: Politik Internasional dan Politik Hukum Nasional Indonesia*. Jakarta: Rajawali pers, halaman 85.

¹⁴ *Ibid.*, halaman 86-87.

¹⁵ Sinta Dewi Rosadi. 2015. *Cyber Law (aspek data privasi menurut hukum internasional, regional, dan nasional)*. Bandung: Refika Aditama, halaman 7.

Cyber Terrorism digambarkan sebagai suatu tindakan terrorisme yang dilakukan dengan menggunakan komputer. Bentuk terrorisme tersebut beralih dari terrorisme yang dilakukan di dunia nyata (fisik) ke dalam bentuk terrorisme melalui dunia maya (*cyber*), atau dengan kata lain *cyber terrorism* itu merupakan kejahatan terrorisme dengan menggunakan ruang maya (*cyber space*) dalam melakukan kejahatannya. *Cyber Terrorism* dapat didefinisikan sebagai berikut:¹⁶

- 1) James A. Lewis mendefinisikan Cyber Terrorism sebagai Penggunaan jaringan computer sebagai sarana untuk melumpuhkan infrastruktur secara nasional, seperti energy, transportasi, untuk menekan/mengintimidasi kegiatan-kegiatan pemerintah atau masyarakat sipil “*The use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government population)*”.
- 2) Menurut Dorothy E. Denning, *cyber terrorism* sebagai “Penyerangan dengan menggunakan komputer atau mengancam, mengintimidasi atau memaksa pemerintahan atau masyarakat, dengan tujuan untuk mencapai target politik, agama atau ideology. Sarana itu cukup untuk menimbulkan rasa takut yang berasal dari tindakan psikis teroris. Serangan itu secara tidak langsung dapat menimbulkan kematian atau cacat badan, kecelakaan pesawat, pencemaran air, dan kelumpuhan ekonomi secara makro. Kerusakan infrastruktur seperti tenaga listrik atau pelayanan keadaan darurat yang dapat disebabkan oleh tindakan terrorisme mayantara”.

¹⁶Eptik Bsikel, “Pengertian *Cyber Terrorism*”, melalui <http://eptikbsikel9.blogspot.co.id/2015/04/pengertian-cyber-terrorism.html>, diakses Kamis, 18 Agustus 2016, pukul 13:20 WIB.

3) Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mendefinisikan terorisme mayantara sebagai suatu tindakan yang dapat meresahkan dan mengganggu stabilitas masyarakat secara umum. Termasuk dalam definisi ini adalah spamming dan abusing. Spamming adalah pengiriman surat elektronik yang berbau iklan kepada seorang pemilik surat elektronik tanpa sepengetahuan yang punya. Selain itu *spamming* juga menunjuk pada penggunaan server orang lain untuk menyerang server target. Sedangkan abusing adalah tindakan penyalahgunaan internet seperti *distributed denial on service*, *hacking*, penghinaan, menyebarkan SARA, dan juga pornografi. Secara umum pengertian cyber terrorism adalah “suatu bentuk kegiatan terencana yang termotivasi secara politis yang berupa serangan terhadap informasi, sistem komputer, program komputer dan data sehingga mengakibatkan kerugian besar serta jatuhnya korban tak berdosa yang dilakukan oleh satu kelompok grup atau perorangan.”

Proses globalisasi dan perkembangan budaya, kemajuan teknologi persenjataan, kemajuan teknologi informasi dan telekomunikasi memicu semakin berkembangnya bentuk-bentuk terorisme, khususnya kejahatan *cyber terrorism*. Argumen ini sesuai dengan pendapat Jean-Jacques Rousseau dalam artikelnya yang dikirim ke Akademi Dijon bahwa kemajuan seni dan ilmu pengetahuan tidak menunjukkan moralitas manusia. Sebagaimana sebuah teori mengatakan, *crime is a product of society itself* yang dapat diartikan bahwa masyarakat itu sendirilah yang melahirkan suatu kejahatan. Semakin tinggi tingkat intelektualitas suatu

masyarakat, maka semakin canggih pula kejahatan yang mungkin terjadi dalam masyarakat tersebut.

Kemajuan teknologi di bidang telekomunikasi dan informasi menjadi sarana penerapan strategi perlawanan kaum teroris secara tidak langsung (*indirect strategi*). Karena sifatnya yang tidak dibatasi ruang dan waktu maka aksi teror dapat dilakukan dimana saja dan kapan saja sebab distribusi geografisnya mencakup seluruh dunia, tidak ada pusat kontrolnya dan kecepatan beroperasi sesuai waktu sesungguhnya (*real time speed*).

Aksi *Cyber terrorism* cenderung lebih murah hanya dengan cukup kemampuan yang memadai maka aksi dapat dilakukan dengan cepat dan memberi hasil yang spektakuler. Para *hacker* dapat membobol komputer milik bank dan memindahkan dan secara melawan hukum atau menggunakan kartu kredit orang lain untuk berbelanja perlengkapan untuk aksi teror melakukan kejahatan pencucian uang dan mengobrak-abrik sistem komputer. Melalui internet, proses komunikasi antar-anggota, koordinasi dan konsolidasi, rekrutmen dan propaganda dapat dengan lebih mudah dilakukan.

Bentuk terorisme beralih dari terorisme yang dilakukan didunia nyata (fisik) kedalam bentuk terorisme melalui dunia maya (*cyber*). Internet digunakan untuk merancang dan melaksanakan serangan terhadap objek-objek sasaran didunia nyata yang memiliki hubungan sistem komputer di mana target dan kerusakan terjadi didunia nyata. Tindak kejahatan ini digolongkan kedalam detik semi online.

1. Karakteristik *Cyber terrorism*

Secara garis besar, *Cyber terrorism* dapat dibagi menjadi dua bentuk atau karakteristik, yaitu sebagai berikut :

- 1) *Cyber terrorism* yang memiliki karakteristik sebagai tindakan teror terhadap sistem komputer, jaringan, dan/atau basis data dan informasi yang tersimpan didalam komputer.
- 2) *Cyber terrorism* berkarakter untuk pemanfaatan Internet untuk keperluan organisasi dan juga berfungsi sebagai media teror kepada pemerintah dan masyarakat.

2. Bentuk-bentuk *Cyber terrorism*

Menurut Cahyana Ahmadjaya kegiatan terrorisme dengan menggunakan teknologi komunikasi dan informasi dilakukan melalui bentuk:¹⁷

1. *Unauthorized Access to Computer System dan Service*. Merupakan kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer.
2. *Carding*. Atau yang disebut dengan *credit card fraud* merupakan tindakan memanfaatkan kartu kredit orang lain untuk berbelanja di toko-toko online guna membeli peralatan terrorisme dan pembiayaan operasional. Teroris mencari nomor-nomor *credit card* orang lain melalui chanel di IRC, melalui *CC Generator*, meng-*hack* toko online dan masuk databasenya, membuat

¹⁷ Dikdik M Arief Mansur dan Elisatris Gultom. 2009. *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama, halaman 67-68.

website palsu mengenai validitas kartu kredit seperti pada umumnya di situs-situs porno.

3. *Email*. Teroris dapat menggunakan email untuk menteror, mengancam dan menipu, spamming dan menyebarkan virus ganas yang fatal, menyampaikan pesan diantara sesama anggota kelompok diantara kelompok .
4. *Cyber Espionage* merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran.
5. *Cyber Sabotage and Extortion*. Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung internet.
6. Membajak media dengan menunggangi satelit dan siaran-siaran TV Kabel untuk menyampaikan pesan-pesannya. Selain itu, teroris dapat mencari metode-metode untuk menyingkap “penyandian” signal-signal TV Kabel yang ada dan menyadap siarannya. Contoh kasus demikian adalah kasus “*Captain Midnight*” memanipulasi siaran HBO yang berjudul “*The Falcon and the Snowman*”.
7. *Phreaker*, merupakan Phone Freaker yaitu kelompok yang berusaha mempelajari dan menjelajah seluruh aspek sistem telepon misalnya melalui nada-nada frekuensi tinggi (*system multy frequency*).
8. *Hacking* untuk merusak sistem dilakukan melalui tahap mencari sistem komputer (*foot printing*) dan mengumpulkan informasi untuk menyusup

seperti mencari pintu masuk (*scanning*). Setelah menyusup, penjelajahan sistem dan mencari akses ke seluruh bagian (*enumeration*) pun dilakukan. Kemudian para hacker membuat *backdoor* dan menghilangkan jejak.

Motif dilakukannya *cyberte rrorism* menurut Zhang ada lima sebab, yaitu:¹⁸

1. *Psychological Warfare*. Menurut Zhang, “*The study of the modern terrorism also reveals one of the most important characteristics of the terrorism is to raise fear.*” Motif ini tidak berbeda dengan motif terorisme konvensional, dimana sasaran utama terorisme adalah menimbulkan rasa ketakutan dalam masyarakat.
2. *Propaganda*. Melalui *cyberterrorism*, kelompok teroris dapat melakukan propaganda tanpa banyak hambatan seperti sensor informasi, karena sifat Internet yang terbuka, upaya ini jauh lebih efektif.
3. *Fundraising*. Melalui *cyberterrorism*, khususnya tindakan penyadapan dan pengambilalihan harta pihak lain untuk kepentingan organisasi teroris telah menjadi motif utama dari *cyberterrorism*. Kelompok teroris juga dapat menambah keuangannya melalui penjualan CD dan buku tentang “perjuangan” mereka.
4. *Communication*. Motif selanjutnya dari *cyberterrorism* adalah komunikasi. Kelompok teroris telah secara aktif memanfaatkan Internet sebagai media komunikasi yang efektif dan jauh lebih aman dibandingkan komunikasi konvensional.

¹⁸ Word Press, “*Cyber Crime Dihubungkan Dengan Tindak Pidana*”, melalui <https://konsultasihukum2.wordpress.com/2010/08/29/cyber-crime-dihubungkan-dengan-tindak-pidana-terorisme/>, diakses Sabtu, 27 Agustus 2016, pukul 01.00.

5. *Information Gathering*. Kelompok teroris memiliki kepentingan terhadap pengumpulan informasi untuk keperluan teror, seperti informasi mengenai sasaran teror, informasi kekuatan pihak musuh, dan informasi lain yang dapat menunjang kinerja kelompok teroris tersebut seperti informasi rahasia (*intelligent information*) terkait persenjataan, dan lainnya. Atas dasar motif *information gathering* lah *cyberterrorism* dilakukan.

Beberapa metode atau cara kerja yang sering digunakan para *cyber terrorist* antara lain :

1. *Spoofing*, yaitu sebuah bentuk kegiatan pemalsuan dimana seorang *hacker* atau *cyber terrorist* memalsukan (*to masquerade*) identitas seorang *user* hingga dia berhasil secara ilegal *logon* atau *login* kedalam satu jaringan komputer seolah-olah seperti *user* yang asli.
2. *Scanner*, merupakan sebuah program yang secara otomatis akan mendeteksi kelemahan (*security weaknesses*) sebuah komputer di jaringan komputer lokal (*local host*) ataupun jaringan komputer dengan lokasi berjauhan (*remote host*). Sehingga dengan menggunakan program ini maka seorang *hacker* yang mungkin secara fisik berada di Inggris dapat dengan mudah menemukan *security weaknesses* pada sebuah *server* di Amerika atau dibelahan dunia lainnya termasuk di Indonesia tanpa harus meninggalkan ruangnya.
3. *Sniffer*, adalah kata lain dari *Network Analyser* yang berfungsi sebagai alat untuk memonitor jaringan komputer. Alat ini dapat dioperasikan hampir

pada seluruh tipe protocol komunikasi data, seperti: *Ethernet, TCP/IP, IPX* dan lainnya.

4. *Password Cracker*, adalah sebuah program yang dapat membuka enkripsi sebuah *password* atau sebaliknya malah dapat mematikan sistim pengamanan *password* itu sendiri.
5. *Destructive Devices*, merupakan sekumpulan program-program virus yang dibuat khusus untuk melakukan penghancuran data-data, diantaranya *Trojan horse, Worms, Email Bombs, Nukes* dan lainnya.

3. Penanganan *Cyber Terrorism*

Perang melawan terorisme harus dilakukan secara komprehensif dengan melakukan pendekatan sektoral dan lintas negara dalam kerangka strategi nasional. Strategi nasional tersebut dapat diuraikan seperti di bawah ini.

Misi nasional dalam pemberantasan terorisme adalah menghentikan aksi terorisme yang mengancam kehidupan bangsa, warga negara dan kepentingan nasional serta menciptakan lingkungan internasional yang tidak menyuburkan terorisme. Untuk memenuhi misi ini maka diperlukan upaya-upaya strategis sebagai berikut :¹⁹

- a) Mengalahkan organisasi teroris dengan menghancurkan persembunyiannya, pemimpinnya, komando, kontrol, komunikasi, serta dukungan materi dan keuangan; kemudian mengadakan kerjasama dan mengembangkan kemitraan baik dari dalam dan luar negeri untuk mengisolasi teroris; mendorong instansi terkait untuk mengembangkan upaya penegak hukum

¹⁹ Dikdik M Arief Mansur dan Elisatris Gultom. *Op. Cit.*, halaman 69-70.

dengan didukung intelejen dan instansi terkait lainnya serta mengembangkan mekanisme penanganan aksi teror dalam suatu sistem terpadu dan koordinasi yang efektif.

- b) Meningkatkan kesiagaan dan kewaspadaan semua komponen bangsa terhadap ancaman terorisme untuk mencegah dijadikannya wilayah tanah air Indonesia sebagai tempat persembunyian para teroris dan tempat tumbuh suburnya ideologi terorisme.
- c) Menghilangkan faktor-faktor korelatif yang dapat dieksploitasi menjadi alasan pembenar aksi teroris seperti kesenjangan sosial, kemiskinan, konflik politik dari SARA.
- d) Melindungi bangsa, warga negara dan kepentingan nasional.

Strategi Implementasi dilakukan melalui upaya represif, preventif, resosialisasi dan pengembangan infrastruktur pendukung. Upaya – upaya tersebut perlu dilakukan secara terpadu sebab penyelesaian yang hanya berdasarkan pada satu konsep saja tidak efektif untuk menghentikan terorisme. Upaya represif antara lain dilakukan melalui perbaikan sistem peradilan dan perundang-undangan, investigasi, intelejen dan militer. Implementasi upaya represif misalnya dilakukan:²⁰

1. Pembentukan Undang-undang *cyber law*, pertukaran informasi dengan negara-negara lain, merevisi undang-undang yang kontra-produktif dalam pemberantasan *cyber terrorism*, memberikan perlindungan saksi, mempercepat proses peradilan, penerapan pengadilan khusus dan penerapan

²⁰ *Ibid.*, halaman 72-73.

pengadilan *in absentia* serta meratifikasi berbagai konvensi internasional. Ratifikasi beberapa konvensi internasional diperlukan sebab dapat memberikan kerangka kerjasama internasional untuk mencegah dan memberantas aksi terorisme yang sifatnya transnasional dan melibatkan bentuk kejahatan terorganisir lainnya. Ratifikasi juga merupakan upaya agar ketentuan perundang-undangan nasional sesuai dengan sistem hukum internasional.

2. Investigasi, Melakukan upaya paksa seperti penangkapan, penahanan, pemeriksaan sesuai ketentuan hukum dengan menghindari terjadinya pelanggaran HAM, kerjasama internasional dalam penyelidikan, kerjasama internasional di bidang teknis laboratorium, *cyber forensic*, *communication forensic*, *surveillance*, dan dukungan teknis lainnya, pelatihan penyidikan, mengungkap jaringan teroris secara tuntas, pembekuan aset organisasi teroris serta kelompok terkait, pelaksanaan undang-undang pencucian uang secara konsisten. Pengumpulan informasi dilakukan berdasarkan KUHAP yang menyatakan bahwa penyelidikan adalah serangkaian tindakan penyidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat tidaknya dilakukan penyelidikan. Ketentuan mengenai penyidikan dalam Pasal 5 ayat (1) KUHAP menyatakan bahwa penyidik berwenang untuk melakukan penyidikan dan atas perintah penyidik dapat melakukan beberapa tindakan demi kepentingan untuk mengumpulkan alat bukti sebanyak – banyaknya. Oleh

karena itu penyidik harus memiliki teknik dan taktik pengumpulan informasi dan barang bukti.

3. Intelejen, Mengembangkan sistem deteksi dini, pertukaran informasi intelejen dengan negara lain, pembangunan database terorisme, deteksi dini pada provokasi ke arah permusuhan bernuansa SARA, kebencian pada kelompok, agama atau negara tertentu. Demi kepentingan mengumpulkan informasi dan barang bukti yang sebanyak-banyaknya maka seorang penyidik harus menguasai teknik dan taktik pengumpulan informasi dan barang bukti.
4. Militer, Serangan ke markas, pembebasan sandera, pengamanan vip dan instalasi vital, menyiapkan pasukan khusus anti-terorisme.

Upaya preventif dilakukan antara lain dengan memberikan larangan penyiaran langsung wawancara dengan teroris, pelarangan publikasi naskah-naskah dan pernyataan teroris yang banyak ditemukan pada website-website kelompok teroris. Upaya resosialisasi dan rehabilitasi antara lain dengan meresosialisasi anggota kelompok melalui pergaulan sosial yang normal. Upaya pengembangan infrastruktur pendukung antara lain dengan memberikan dukungan berupa bantuan internasional dan pengadaan peralatan dan teknologi bagi Polri, Intelejen, TNI dan fasilitas koordinasi (Desk KPT), peningkatan satuan-satuan pelaksanaan lapangan dan jajaran penegak hukum.

Network Manager atau *System Administrator* tentu memerlukan berbagai peralatan (*tools*) untuk membantu mengamankan jaringan komputernya. Beberapa *tools* bahkan memang dibuat khusus dalam rangka melakukan *testing* sistem

jaringan untuk mengetahui kekuatan dan kelemahan dari sebuah sistem jaringan komputer. *Tools* tersebut antara lain:

1. *SATAN (Security Administrator's Tool for Analysing Network)*, peralatan yang dibutuhkan untuk melakukan analisa sistem jaringan komputer secara menyeluruh sehingga *performance* sekaligus titik kelemahan dari jaringan komputer tersebut dapat diketahui.
2. *TCP Wrapper* untuk memonitor jaringan komputer (*trafficking*) terutama dalam hal lalu lintas paket data dalam jaringan yang menggunakan protokol TCP/IP (*internet protocol*) sehingga paket data yang lewat dapat dipantau dengan baik.
3. *Crack* untuk melakukan *password security testing* dimana manfaatnya untuk mengetahui kelemahan dari password para pengguna, karena tidak semua pengguna tahu cara membuat password yang aman. Bahkan ada yang tidak menggunakannya sama sekali.
4. *Firewall*, adalah sebuah sistem proteksi untuk melaksanakan pengawasan lalu lintas paket data yang menuju atau meninggalkan sebuah jaringan komputer. Sehingga paket data yang telah diperiksa dapat diterima atau ditolak bahkan dimodifikasi terlebih dahulu sebelum memasuki atau meninggalkan jaringan tersebut.

Kebebasan atas informasi dan komunikasi tidak bersifat mutlak. Apabila di lihat dari ajaran aliran filsafat hukum kodrat mengenai hak milik maka hak untuk melakukan komunikasi dan hak atas informasi sebenarnya merupakan kewajiban sekaligus hak manusia untuk mempertahankan hidup manusia. Kodrat

individual harus harmonis dengan kodrat sosial. Hak individual harus bersifat fungsi sosial dan tidak merusak atau merugikan individu lain dan masyarakat. *Cyberspace* sebagai ruang elektronik berisi masyarakat virtual yang terbentuk melalui jalinan komunikasi dalam sebuah jaringan komputer harus di manfaatkan oleh tiap individu dan kelompok guna kelangsungan hidupnya.

Aksi Terorisme merupakan tindakan seorang atau sekelompok orang yang ingin mempertahankan hidup individu dan kolektif kelompoknya dengan cara mengancam dan membahayakan kelangsungan hidup orang lain. Oleh karena itu, tindakan kejahatan teroris harus dilarang dan pelakunya di hukum menurut ketentuan hukum yang berlaku.

Jika disepakati bahwa kejahatan *cyber terrorism* digolongkan sebagai tindakan kejahatan yang harus dihukum, pertanyaan yang diajukan adalah apakah perundang-undangan Indonesia sudah mengatur masalah tersebut? Ada dua kelompok pendapat dalam menjawab pertanyaan ini. Kelompok *pertama* berpendapat bahwa sampai hari ini belum ada perundang-undangan yang mengatur masalah *cyber terrorism*. Oleh karenanya akan sulit bagi aparat penegak hukum untuk menghukum pelakunya. *Kelompok Kedua* beranggapan bahwa tidak ada kekosongan hukum dan para penegak hukum dapat menggunakan ketentuan hukum yang sudah ada. Mengingat lamanya penanganan tindakan kejahatan *cyber terrorism* tidak dapat ditunda maka hakim harus melakukan penemuan hukum melalui penafsiran dan konstruksi hukum.

Menanggulangi atau biasa disebut penanganan adalah proses, cara, satu atau serangkaian proses pekerjaan. Penanggulangan tindak kejahatan internet

(*cyber crime*) terdapat pada kepolisian sebagai pembuat kebijakan, penyedia fasilitas pelayanan, dan sebagai pengawas dibidang Informasi dan Transaksi elektronik kota Medan. Dalam bukunya, Prof. Barda Nawawi Arief mengungkapkan beberapa upaya penanggulangan *cyber crime* yaitu:

1. *Cyber crime* harus dikriminalisasikan.
2. Diperlukan sarana penal.
3. Diperlukan kerjasama antara pemerintah dan industri terhadap tujuan umum pencegahan dan penanggulangan kejahatan komputer agar internet menjadi sarana yang aman.
4. Diperlukan kerja sama internasional untuk menelusuri/ mencari penjahat di internet.²¹

Sedangkan dalam penelitiannya Suharyo mengemukakan beberapa hal yang harus dilakukan dalam penanggulangan kejahatan internet yaitu:

1. Peningkatan dan pematapan aparaturn penegak hukum, meliputi pematapan organisasi, personil dan sarana untuk penyelesaian perkara pidana.
2. Perundang-Undangan yang dapat berfungsi menganalisis dan membendung kejahatan dan mempunyai jangkauan kemasa depan.
3. Mekanisme peradilan pidana yang efektif dan memenuhi syarat cepat, tepat murah dan sedernhana.
4. Koordinasi antar aparaturn penegak hukum dan aparaturn pemerintahan lainnya yang berhubungan untuk meningkatkan daya guna dalam penanggulangan kriminalitas.

²¹ Barda Nawawi Arief, *Op. Cit.*, halaman 7.

5. Partisipasi masyarakat untuk membantu kelancaran pelaksanaan penanggulangan kriminalitas.²²

C. Tindak Pidana

Istilah tindak pidana berasal dari istilah yang dikenal dalam hukum pidana Belanda yaitu *Strafbaar Feit*.²³ *Strafbaar Feit*, terdiri dari tiga kata, yakni *Straf*, *Baar*, dan *Feit*. Dari tujuh istilah yang digunakan sebagai terjemahan dari *Strafbaar Feit* itu, ternyata *Straf* diterjemahkan dengan pidana dan hukum. Perkataan *Baar* diterjemahkan dengan dapat dan boleh. Sementara itu, untuk kata *Feit* diterjemahkan dengan tindak, peristiwa, pelanggaran, dan perbuatan.²⁴

Tindak pidana merupakan perilaku yang menyimpang dari hukum yang dibuat atau perbuatan yang bertentangan dengan peraturan hukum yang berlaku, bebarapa pendapat para ahli sarjana Barat mengenai tindak pidana:

1. Pompe

Perkataan tindak pidana (*Strafbaar Feit*) itu secara teoritis dapat dirumuskan sebagai “suatu pelanggaran norma (gangguan terhadap tertib hukum) yang dengan sengaja atau tidak dengan sengaja telah dilakukan oleh seorang pelaku, dimana penjatuhan hukuman terhadap pelaku tersebut adalah perlu demi terpeliharanya tertib hukum dan terjaminnya kepentingan umum”.

²² Suharyo. 2012. *Penelitian Hukum Tentang Penerapan bantuan Timbal Balik Dalam Masalah Pidana Terhadap Kasus-kasus Cybercrime*. Cililitan: BPHN Kemenkumham RI, halaman 8.

²³ Adami Chazawi. 2002. *Pelajaran Hukum Pidana Bagian I*. Jakarta: Rajawali pers, halaman 67.

²⁴ *Ibid.*, halaman 69.

2. Simons

Merumuskan tindak pidana (*Strafbaar Feit*) itu sebagai suatu “tindakan melanggar hukum yang telah dilakukan dengan sengaja ataupun dengan tidak sengaja oleh seseorang yang dapat dipertanggungjawabkan atas tindakannya dan yang oleh Undang-Undang telah dinyatakan sebagai suatu tindakan yang dapat dihukum”.

3. Hazewinkel-Suringa

Mereka merumuskan tindak pidana (*Strafbaar Feit*) sebagai “suatu perilaku manusia yang pada suatu saat tertentu telah ditolak didalam sesuatu pergaulan hidup tertentu dan dianggap sebagai perilaku yang harus ditiadakan oleh hukum pidana dengan menggunakan sarana-sarana yang bersifat memaksa yang terdapat di dalamnya”.

4. Van Hattum

Merumuskan tindak pidana (*Strafbaar Feit*) adalah “tindakan, yang karena telah melakukan tindakan semacam itu membuat seseorang menjadi dapat dihukum”.

5. Van Hamel

Merumuskan tindak pidana (*Strafbaar Feit*) adalah “suatu serangan atau suatu ancaman terhadap hak-hak orang lain”.²⁵

Banyak juga para ahli hukum Indonesia yang mengartikan apa itu tindak pidana (*strafbaar feit*) salah satunya adalah:

²⁵ P.A.F. Lamintang. *Op. Cit.*, halaman 181-185.

1. Moeljatno yang mengartikan Tindak Pidana adalah perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman atau sanksi yang berupa pidana tertentu, bagi barang siapa yang melanggar larangan tersebut.
2. Simons dalam buku Mahrus Ali, Tindak Pidana adalah suatu tindakan melanggar hukum yang telah dilakukan dengan sengaja ataupun tidak dengan sengaja oleh seseorang yang dapat dipertanggungjawabkan atas tindakannya yang oleh Undang-Undang telah dinyatakan sebagai suatu tindakan yang dapat dihukum.²⁶
3. Utrecht menganjurkan pemakaian istilah peristiwa pidana, karena istilah peristiwa itu meliputi perbuatan (*handelen* atau *doen positief*) atau melalaikan (*verzuim* atau *naletan* atau *niet-doen, negatief*) maupun akibatnya.²⁷
4. Satochid Kartanegara dalam rangkaian kuliah beliau menganjurkan pemakaian istilah tindak pidana, karena istilah tindak (tindakan), mencakup pengertian melakukan atau berbuat (*active handeling*) dan/atau pengertian tidak melakukan, tidak berbuat, tidak melakukan suatu perbuatan (*passieve handeling*). Istilah perbuatan berarti melakukan, berbuat (*actieve handeling*) tidak mencakup pengertian mengakibatkan, tidak melakon. Istilah peristiwa, tidak menunjukkan kepada hanya tindakan manusia. Sedangkan terjemahan pidana untuk *Strafbaar* adalah sudah tepat.²⁸

²⁶ Mahrus Ali. 2015. *Asas-Asas Hukum Pidana Korporasi*. Jakarta: Raja Grafindo, halaman 52.

²⁷ E.Y Kanter dan S.R. Sianturi. 2012. *Asas-Asas Hukum Pidana Di Indonesia Dan Penerapannya*. Jakarta: Stora Grafika, halaman 208.

²⁸ *Ibid.*

Sebelum dicoba memberikan perumusan tindak pidana, terlebih dahulu akan disetir beberapa perumusan yang telah diperkenalkan oleh beberapa sarjana kita sebagai berikut:

1. Moeljatno

Setelah memilih perbuatan pidana sebagai terjemahan dari *Strafbaar Feit*, beliau memberi perumusan (pembatasan) sebagai suatu perbuatan yang dilarang dan diancam dengan pidana barang siapa yang melanggar larangan tersebut dan perbuatan itu harus pula betul-betul dirasakan oleh masyarakat sebagai perbuatan yang tak boleh atau menghambat akan tercapainya tata dalam pergaulan masyarakat yang dicita-citakan oleh masyarakat itu. Makna perbuatan pidana, secara mutlak harus termaktub unsur formil, yaitu mencocoki rumusan Undang-Undang (*Tatbestandmatigheit*) dan unsur materil, yaitu sifat bertentangnya dengan cita-cita mengenai pergaulan masyarakat atau dengan pendek, sifat melawan hukum (*Rechtswiridigkeit*).

2. R. Tresna

Setelah mengemukakan bahwa sungguh tidak mudah memberikan suatu ketentuan atau defenisi yang tepat, mengatakan bahwa: peristiwa pidana itu ialah suatu perbuatan atau rangkaian perbuatan manusia, yang bertentangan dengan Undang-Undang atau peraturan-peraturan lainnya, terhadap perbuatan mana diadakan tindakan penghukuman. Beliau menerangkan bahwa perumusan tersebut jauh daripada sempurna, karena dalam uraian beliau selanjutnya diutarakan bahwa sesuatu perbuatan itu baru dapat dipandang sebagai peristiwa pidana, apabila telah memenuhi segala syarat yang diperlukan.

3. Wirjono Prodjodikoro

Merumuskan tindak pidana berarti suatu perbuatan yang pelakunya dapat dikenakan hukuman pidana. Dan pelaku itu dapat dikatakan merupakan “*Subject*” tindak pidana.²⁹

Manakala tindak pidana dikonsepsikan sebagai perbuatan yang dilarang dan diancam dengan pidana barang siapa yang melakukannya, maka unsur-unsur tindak pidana meliputi 3 (tiga) hal:

- 1) Perbuatan itu berwujud suatu kelakuan baik aktif maupun pasif yang berakibat pada timbulnya suatu hal atau keadaan yang dilarang oleh hukum.
- 2) Kelakuan dan akibat yang timbul tersebut harus bersifat melawan hukum baik dalam pengertiannya yang formil maupun yang materil.
- 3) Adanya hal-hal atau keadaan tertentu yang menyertai terjadinya kelakuan dan akibat yang dilarang oleh hukum.³⁰

Seseorang yang dapat dipertanggungjawabkan tindak pidana harus memenuhi unsur-unsur di atas, Terlibatnya dalam tindak pidana juga diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang terdapat dalam Pasal 55 yang dimana isinya berkesimpulan subjek yang bagaimana saja dapat dikatakan terlibat dalam tindak pidana yang dijelaskan sebagai berikut:

1. Orang yang melakukan (*dader plagen*)

Orang ini ialah seorang yang sendirian telah berbuat mewujudkan segala anasir atau elemen dari peristiwa pidana. Dalam peristiwa pidana yang dilakukan dalam jabatan misalnya orang itu harus pula memenuhi elemen “status sebagai pegawai negeri”.

²⁹*Ibid.*, halaman 208-209.

³⁰*Ibid.*, halaman 55.

2. Orang yang menyuruh melakukan (*doen plagen*)

Disini sedikitnya ada dua orang yang menyuruh (*doen plagen*) dan yang disuruh (*pleger*). Jadi bukan orang itu sendiri yang melakukan peristiwa pidana, akan tetapi ia menyuruh orang lain, meskipun demikian *tochia* dipandang dan dihukum sebagai orang yang melakukan sendiri yang melakukan peristiwa pidana, akan tetapi ia menyuruh orang lain, disuruh (*pleger*) itu harus hanya merupakan suatu alat (*instrument*) saja, maksudnya ia tidak dapat dihukum karena tidak dapat dipertanggungjawabkan atas perbuatannya, misalnya dalam hal-hal sebagai berikut:

- a. Tidak dapat dipertanggungjawabkan menurut Pasal 44, Umpamanya A berniat akan membunuh B, tetapi karena tidak berani melakukan sendiri, telah menyuruh C (seorang gila) untuk melemparkan granat tangan kepada B, bila C betul-betul telah melemparkan granat itu, sehingga B mati, maka C tidak dapat dihukum karena tidak dapat dipertanggungjawabkan, sedang yang dihukum sebagai pembunuh ialah A.
- b. Telah melakukan perbuatan itu karena terpaksa oleh kekuasaan yang tidak dapat dihindarkan (*overmacht*) menurut Pasal 4, Umpamanya A berniat membakar rumah B dan dengan menodong pakai pistol menyuruh C supaya membakar rumah itu. Jika C menurut membakar rumah itu, ia tidak dapat dihukum karena dipaksa, sedangkan A meskipun tidak membakar sendiri, *toch* dihukum sebagai pembakar.
- c. Telah melakukan perbuatan itu atas perintah jabatan yang tidak sah menurut Pasal 51, misalnya seorang Inspektur Polisi mau membalas dendam pada

seorang musuhnya dengan memasukkan orang itu dalam kamar tahanan. Ia menyuruh B seorang agen Polisi dibawah perintahnya supaya menangkap dan memasukkan dalam tahanan orang tersebut dengan dikatakan bahwa orang itu tersangka mencuri. Jika B melaksanakan suruhan itu, ia tidak dapat dihukum atas merampas kemerdekaan orang karena ia menyangka bahwa perintah itu sah, sedang yang dihukum sebagai perampas kemerdekaan ialah tetap si Inspektur Polisi.

- d. Telah melakukan perbuatan itu dengan tidak ada kesalahan sama sekali, misalnya A berniat akan mencuri sepeda yang sedang ditaroh di muka kantor Pos. Ia tidak berani menjalankan sendiri, tetapi ia dengan menunggu agak jauh minta tolong pada B untuk mengambilkan sepeda itu dengan dikatakan bahwa itu dalah miliknya. Jika B memenuhi permintaan itu, ia tidak salah mencuri, karena elemen “sengaja” tidak ada. Yang dihukum sebagai pencuri tetap A.

3. Orang yang turut melakukan (*mede plagen*)

Turut melakukan dalam arti kata “bersama-sama melakukan”. Sedikit-dikitnya harus ada dua orang, ialah orang yang melakukan (*pleger*) dan orang turut melakukan (*medepleger*) peristiwa pidana itu. Disini diminta, bahwa kedua orang itu semuanya melakukan perbuatan pelaksanaan, jadi melakukan anasir atau elemen peristiwa pidana itu. Tidak boleh misalnya hanya melakukan perbuatan persiapan saja atau perbuatan yang sifatnya hanya menolong, sebab jika demikian, maka orang yang menolong itu tidak masuk “*medepleger*” akan tetapi dihukum sebagai “membantu melakukan” (*medeplichtige*) tersebut

dalam Pasal 56. Contoh : A berniat mencuri dirumah B dan mengajak C untuk bersama-sama melakukan. Kedua-duanya masuk rumah dan mengambil barang-barang, atau C yang menggali lubang “gasiran”, sedang A yang masuk dan mengambil barang-barangnya. Disini C dihukum sebagai “*medepleger*”, karena melakukan perbuatan pelaksanaan pencurian itu. Andai kata C hanya berdiri diluar untuk menjaga dan memberi isyarat kalau ada orang datang, maka C dihukum sebagai “*medeplichtige*” Pasal 56 sebab perbuatannya hanya bersifat menolong saja.

4. Orang yang dengan pemberian, salah memakai kekuasaan, memakai kekerasan dengan sengaja membujuk melakukan perbuatan itu (*uitlokker*).

Orang itu harus sengaja membujuk orang lain, sedang membujuknya harus memakai salah satu dari jalan-jalan seperti dengan pemberian, salah memakai kekuasaan dan sebagainya. Yang disebutkan dalam Pasal itu, artinya tidak boleh memakai jalan lain. Disini seperti halnya dengan “suruh melakukan” sedikit-dikitnya harus ada dua orang, ialah orang yang membujuk dan yang dibujuk, hanya bedanya pada “membujuk melakukan” orang yang dibujuk itu dapat dihukum juga sebaga “*pleger*” sedang pada “suruh melakukan”, orang yang disuruh itu tidak dapat dihukum.

Berdasarkan hal di atas orang-orang yang dapat diberikan pertanggungjawaban dalam melakukan tindak pidana sesuai dengan aturan Pasal 55 Kitab Undang-Undang Hukum Pidana (KUHP), dengan demikian tidak sembarang orang yang dapat dijadikan tersangka dalam perbuatan tindak pidana

harus sesuai dan diselidiki oleh Kepolisian yang dapat dijadikan tersangka dalam perbuatan tindak pidana kejahatan.

BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Pengaturan Hukum Terhadap Pelaku *Cyber Terrorism* Menurut Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme

Tindak pidana *Cyber terrorism* merupakan kejahatan yang dilakukan dengan menggunakan alat teknologi berupa komputer di ruang maya (*cyberspace*) dengan unsur utamanya melakukan kegiatan teror, propaganda, koordinasi dari jarak jauh dan dengan menebarkan kebencian (*hate teror*), menghimpun dana, perekrutan, pelatihan dan perencanaan secara terorganisir yang melewati batas negara, hingga menjadi kejahatan di dunia maya (*cyber crime*). Tindakan melawan hukum yang dilakukan setiap orang dan atas nama kelompok tertentu ini di *cyberspace* mengakibatkan timbulnya korban jiwa dan materiil yang besar terhadap keamanan orang lain, atas upaya penyerangan pada sistem komputer yang merusak data, sistem komputer serta infrastruktur vital.

The british law commission misalnya, mengartikan "*computer fraud*" sebagai manipulasi komputer dengan cara apapun yang dilakukan dengan iktikad buruk untuk memperoleh uang, barang atau keuntungan lainnya atau dimaksudkan untuk menimbulkan kerugian kepada pihak lain. Mandel membagi "*computer crime*" atas dua kegiatan, yaitu:

1. Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian, atau penyembunyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan dan pelayanan.

2. Ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras dan lunak, sabotase dan pemerasan.³¹

Dengan demikian jelas sudah *cyber terrorism* sebagai kejahatan di ruang maya (*cybercrime*) perlu ditegaskan pengaturan hukumnya dalam Hukum Nasional Indonesia, agar dapat dipidanakan atas pertanggungjawaban hukum bagi setiap orang dan atau kelompok tertentu dengan sengaja melakukan aksi kejahatan di ruang maya yang menyebabkan terganggunya keamanan terhadap orang lain dengan pembuktian unsur elektronika yang ada.

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

Serangan teroris langsung ditanggapi dengan bermunculan dan penerapan produk hukum pemberantasan terorisme. Munculnya produk pidana terhadap pelaku teror terlihat sesaat sebagai penyelesaian yang utama. Pemerintah merasa telah berhasil, bila dalam suatu serangan teror, individu pelakunya dapat segera ditangkap dan diproses secara hukum.³²

Indonesia sebagai negara hukum yang ditegaskan dalam Pasal 1 Ayat (3) UUD 1945 dalam konteks Konstitusi Negara, telah merespon terjadinya percepatan kebutuhan akan antisipasi permasalahan hukum akibat perilaku hukum

³¹ Budi suhariano, *Op. Cit.*, halaman 10.

³² Petrus Reinhard Golose. 2009. *Deradikalisasi Terorisme: Humanis, Soul Approach dan Menyentuh Akar Rumpit*). Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian, halaman 115.

menyimpang dalam menggunakan komputer dan berinteraksi untuk melakukan kejahatan.

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

Pengaturan mengenai *cyber terrorism* dalam *cyber law* diharapkan bisa memberikan kepastian tegas dalam penjelasan hukum mengenai pengaturan kejahatan *cyber terrorism* secara khusus. Tentunya memiliki alasan utama yaitu adanya aspek yang terkait dengan kejahatan tindak pidana *cyber terrorism* yang dipertegas secara komprehensif dalam sebuah ketentuan undang-undang *cyber law* yang mengatur pergerakan dan penggunaan serta penyimpangan dalam tindakan kejahatan *cyber* yang menggunakan komputer sebagai alat utama dan kemanfaatan dari media teknologi yang berkembang.

Artinya tidak hanya bergantung pada satu Undang-Undang (*umbrella act*) saja, meski kita tahu telah ada Undang-Undang Nomor 15 Tahun 2003, ataupun Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi, atau Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Memang secara yuridis dalam penyelesaian masalah hukum tindak pidana *cyber*

terrorism ini hakim yang menangani harus melakukan penemuan hukum melalui penafsiran dan konstruksi hukum. Namun demikian bila pembangunan hukum nasional mengapresiasi hadirnya *cyber law* secara terintegrasi akan menjadi sebuah penguatan kepastian hukum yang lebih baik, mengingat banyak sekali gerakan terkait tindak pidana terorisme semakin berkembang dengan berbagai pola komunikasi dalam pemanfaatan media yang ada, sebagai alat komunikasi untuk melakukan aksi kejahatannya.

Ketentuan Undang-Undang Nomor 15 Tahun 2003 tentang Terorisme dapat digunakan untuk menjerat pelaku *Cyber Terrorism* karena terdapat Pasal yang mengatur tindak pidana terorisme pada ketentuan Pasal 6, Pasal 7, Pasal 9, Pasal 11 dan Pasal 12. Pada ketentuan Undang-Undang ini dinyatakan bahwa seseorang dianggap melakukan aksi terorisme dan dapat dijatuhi hukuman walaupun tindak pidana terorisme belum terjadi atau baru hanya sampai pada tahap dengan maksud atau dengan tujuan atau merencanakan tindak pidana terorisme.

Mengetahui seseorang atau sekelompok orang memiliki maksud dan rencana melakukan tindak pidana terorisme tentunya pihak penyidik harus mendapatkan barang bukti guna mendukung dugaan tersebut bila ternyata telah ada niat dalam upaya tindak pidana terorisme. Ketentuan Pasal 27 Undang-Undang Nomor 15 Tahun 2003, telah menyatakan berbagai macam alat bukti, dan satu diantaranya menyebutkan adanya alat bukti elektronik sebagai alat bukti yang sejajar dan sah sebagaimana dimaksud dalam hukum Acara Pidana.

Sejajar dengan pembuktian itu disebutkan juga dalam ketentuan Pasal 184 KUHAP bahwa alat bukti itu adalah berupa Informasi yang diucapkan, dikirimkan, disimpan secara elektronik dengan menggunakan alat optik seupa dengan hal itu yaitu data, rekaman, atau informasi yang dapat dilihat, dibaca, dan atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada tulisan, suara atau gambar, peta, rancangan, foto, atau sejenisnya, huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat difahami oleh orang yang mampu membaca atau memahaminya.

Akan tetapi persoalannya tidak semudah yang kita fahami. Itu dikarenakan ada permasalahan dalam kesulitan keterukuran untuk mengetahui niat seseorang merencanakan, bermaksud dan bertujuan melakukan aksi terorisme. Analisa yang tajam dalam hal penyalahgunaan alat komputer dalam bentuk komunikasi dan informasi yang berkembang tidak boleh meleset hingga terjadi salah tangkap. Aparat hukum dalam hal ini penegak hukum yang berwenang harus benar-benar dapat menganalisa secara validitas terkait penggunaan alat-alat bukti elektronik yang digunakan untuk komunikasi secara elektronik apakah itu telah digunakan penyalahgunaan atau tidak dengan alat komputer dengan program internet.

Abdul Hakim G menyampaikan terkait upaya pembuktian bahwa seseorang atau kelompok tertentu melakukan tindak pidana *cyber terrorism* dalam investigasi terorisme, maka penting kiranya kita melihat beberapa ketentuan yang terdapat pada Undang-undang Patriot Amerika Serikat, yang bisa menjadi

perbandingan dalam penciptaan Undang-undang terkait dengan *cyber terrorism* atau kejahatan terorisme di ruang maya. Undang-Undang Patriot Amerika Serikat itu diantaranya mengatur mengenai:³³

1. Ketentuan *roving wiretap* agar departemen kehakiman memiliki kekuasaan untuk menyadap guna menelusuri jejak para tersangka tanpa mengindahkan telepon yang mereka gunakan.
2. Memperkenalkan sharing informasi yang semula dilindungi oleh *grand jury* di antara aparat intelejen dan aparat penegak hukum.
3. Memperkenankan penyitaan pesan-pesan *voicemail* sesuai dengan surat perintah (*warrant*)
4. Meningkatkan kekuasaan untuk menelusuri jejak para tersangka melalui internet.
5. Mensyaratkan pembukaan (*disclosure*) komunikasi para pelanggan atau catatan oleh para provider pelayanan komputer di daerah yang jauh (*remote*) dan pelayanan jasa komunikasi elektronik seperti ISPs kepada publik tanpa ditunda jika penyedia jasa (*provider*) mempunyai alasan yang dapat dipercaya adanya suatu yang membahayakan secara langsung atau mematikan atau melukai secara fisik.
6. Memberikan kekebalan (*immunity*) kepada provider jasa komunikasi elektronik atau *wire* atau orang yang menyediakan informasi, fasilitas atau bantuan teknis sesuai perintah atau permintaan pengadilan guna memberi bantuan darurat.

³³ Dikdik M Arief Mansur dan Elisatris Gultom. *Op., Cit*, halaman 78-79.

7. Mele vbgalisasi tindakan aparat penegak hukum untuk menangkap (*intercept*) komunikasi elektronik atau *wire* dari penyalahgunaan komputer dan memiliki alasan untuk meyakini isi komunikasi tersebut relevan bagi penyelidikan.
8. Memuat ketentuan matahari terbenam (*sunset principle*) di mana beberapa ketentuan yang berkenaan dengan pengawasan akan berakhir.

Ketentuan Undang-undang Patriot Amerika Serikat di atas hanyalah sebagai pembanding. Negara Indonesia telah memiliki Undang-undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme yang pada saat kelahiran undang-undang tersebut dijiwai dengan semangat proteksi kedaulatan negara, proteksi HAM bagi tersangka/terdakwa, dan juga proteksi terhadap korban-korban terorisme serta fasilitas publik.

Keabsahan transaksi dan kekuatan pembuktian, transaksi elektronik tidak memerlukan *hardcopy* atau warkat kertas, namun demikian setiap transaksi yang melibatkan eksekusi diberikan tanda bukti berupa nomer/kode yang dapat disimpan/direkam dikomputer atau dicetak.³⁴

Pada dasarnya permasalahan ini bukan permasalahan yang luar biasa dari kaca mata hukum pidana karena hukum pidana yang ada (KUHP) dapat digunakan untuk menanggulangi serta membawa para pelaku pemboman ke muka pengadilan. Tetapi dibalik permasalahan itu muncul pemberian nama atas perbuatan itu dengan sebutan “terrorisme” sehingga menimbulkan persoalan hukum.

³⁴ *Ibid*, halaman 109 .

Masalah yang timbul akibat dari kejahatan dunia maya tidak jauh seperti yang terjadi di dunia fisik. Para penjahat melihat karakteristik internet sebagai kesempatan atau sarana bagi mereka untuk melaksanakan niat jahat melalui berbagai perbuatan yang lebih dikenal dengan *cyber crimes*. Kebebasan untuk berekspresi digunakan untuk menyebarkan informasi yang berisi fitnah, kebebasan untuk mengembangkan teknologi dan kreativitas digunakan untuk merusak website atau menyebarkan virus.³⁵

Persoalan hukum yang timbul adalah bahwa perangkat hukum yang ada tidak dapat digunakan untuk menuntut para pelaku peledakan bom tersebut ke depan pengadilan, seolah-olah ada kekosongan hukum mengenai terorisme. Kepentingan hukum yang dibahayakan oleh tindakan terorisme tidak hanya berupa jiwa dan harta benda, tetapi juga rasa takut masyarakat, kebebasan pribadi, integritas nasional, kedaulatan negara, fasilitas internasional, instalasi publik, lingkungan hidup, sumber daya alam nasional, serta sarana transportasi dan komunikasi.

Terrorisme dapat terjadi kapan saja dan dimana saja serta mempunyai jaringan yang sangat luas sehingga merupakan ancaman terhadap perdamaian dan keamanan, baik nasional maupun internasional. Berkaitan dengan permasalahan terorisme tersebut dibentuklah suatu Perpu Nomor 1 Tahun 2002 yang berlakunya tidak serta merta dan tidak secara otomatis. Sebagai pelaksana ketentuan Perpu Nomor 1 Tahun 2002, pemerintah menerbitkan Perpu Nomor 2 Tahun 2002 tentang pemberlakuan Perpu Nomor 1 Tahun 2002.

³⁵ Josua Sitompul. 2012. *Cyberspace, cybercrimers, cyberlaw*. Jakarta: Tatanusa, halaman 36.

Perpu Nomor 2 tahun 2002 ini dengan Undang-undang Nomor 16 Tahun 2003 ditingkatkan menjadi Undang-undang, sedangkan Perpu Nomor 2 Tahun 2002 tentang Pemberantasan Tindak Pidana Terrorisme ditingkatkan menjadi Undang-undang Nomor 15 Tahun 2003 (selanjutnya disingkat UU terorisme). Sistem perumusan tindak pidana dalam Undang-undang Tindak Pidana Terrorisme Ketentuan pidana dalam Undang-undang Nomor 15 tahun 2003 jo Perpu Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terrorisme terdapat dalam Bab III Pasal 6 sampai dengan Pasal 19, berikut beberapa perumusan Pasal dan ketentuan pidana tersebut

Pasal 6

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

Pasal 9

Setiap orang yang secara melawan hukum memasukkan ke Indonesia, membuat, menerima, mencoba memperoleh, menyerahkan atau mencoba menyerahkan, menguasai, membawa, mempunyai persediaan padanya atau mempunyai dalam miliknya, menyimpan, mengangkut, menyembunyikan, mempergunakan, atau mengeluarkan ke dan/atau dari Indonesia sesuatu senjata api, amunisi, atau sesuatu bahan peledak dan bahan-bahan lainnya yang berbahaya dengan maksud untuk melakukan tindak pidana terorisme, dipidana dengan pidana mati atau penjara seumur hidup atau pidana penjara paling singkat 3 (tiga) tahun dan paling lama 20 (dua puluh) tahun.

Pasal 11

Dipidana dengan pidana penjara paling singkat 3 (tiga) tahun dan paling lama 15 (lima belas) tahun, setiap orang yang dengan sengaja menyediakan atau mengumpulkan dana dengan tujuan akan digunakan atau patut diketahuinya akan digunakan sebagian atau seluruhnya untuk

melakukan tindak pidana terorisme sebagaimana dimaksud dalam Pasal 6, Pasal 7, Pasal 8, Pasal 9, dan Pasal 10.

Pasal 14

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

Pasal 15

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

Pasal 17

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

Pasal 18

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

Pasal 19

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

Melihat berbagai ketentuan yang telah dikriminalisasikan dalam Undang-undang Pemberantasan Tindak Pidana Terrorisme tersebut, nampak adanya kriminalisasi terhadap perbuatan-perbuatan yang berhubungan dengan penyalahgunaan penggunaan internet, yang berbentuk tindak pidana *cyber terrorism*.

Melihat perumusan ketentuan pidana dalam Undang-undang Informasi dan Transaksi Elektronik (ITE) sebagai mana diatur dalam Pasal 45 sampai dengan Pasal 52 maka dapat diidentifikasi bahwa pelaku tindak pidana atau yang dapat dimintakan pertanggungjawaban pidana dalam Undang-undang Informasi dan Transaksi Elektronik (ITE) adalah meliputi individu/orang per orang dan korporasi. Ini terbukti dari ketentuan pasal-pasal tersebut yang diawali dengan kata “Setiap orang” dan “korporasi”.

Masalah pertanggungjawaban pidana berkaitan erat dengan pelaku tindak pidana. Pelaku yang dapat dipidana adalah orang dan korporasi, yang dijelaskan dalam Pasal 1 sub 21 dan dalam ketentuan pidana Undang-undang Informasi dan Transaksi Elektronik (ITE) tersebut. Undang-undang Informasi dan Transaksi Elektronik (ITE) mengatur secara lanjut dan terperinci tentang ketentuan pertanggungjawaban pidana terhadap korporasi, karena Undang-undang Informasi dan Transaksi Elektronik (ITE) tersebut membedakan pertanggungjawaban pidana terhadap individu dan korporasi, sebagaimana yang tercantum dalam Pasal 52 Undang-undang Informasi dan Transaksi Elektronik (ITE).

B. Faktor Penyebab Marak Terjadinya *Cyber Terrorism*

Pada masa awalnya, *cyber crime* didefinisikan sebagai kejahatan komputer. Mengenai kejahatan komputer sendiri, sampai sekarang para sarjana belum sependapat mengenai pengertian atau definisi dari kejahatan komputer. Bahkan penggunaan istilah tindak pidana untuk kejahatan komputer dalam bahasa Inggris pun masih belum seragam. Beberapa sarjana menggunakan istilah “*computer misuse*”, “*computer assisted crime*”, atau “*computer crime*”. Namun para sarjana pada waktu itu, pada umumnya lebih menerima pemakaian istilah “*computer crime*” oleh karena dianggap lebih luas dan biasa dipergunakan dalam hubungan internasional.³⁶ Kejahatan *cyber crime* telah diambil para pelaku teroris sebagai teknik mereka dalam melakukan tindak kejahatan atau sekarang dikenal dengan *cyber terrorism*.

Kejahatan internet (*cyber crime*) terdiri dari berbagai macam cara yang bisa terjadi. Menurut motifnya, kejahatan di internet terbagi atas dua motif yaitu:³⁷

1. Motif Intelektual

Yaitu kejahatan yang dilakukan hanya untuk kepuasan pribadi dan menunjukkan bahwa dirinya mampu untuk mereayasa dan mengimplementasikan di bidang teknologi.

2. Motif Ekonomi, politik, dan kriminal

Yaitu kejahatan yang dilakukan untuk keuntungan pribadi atau golongan tertentu yang berdampak pada kerugian secara ekonomi dan politik pihak lain.

³⁶ Budi Suharianto. *Op., Cit*, halaman 9.

³⁷ Aji Supriyanto. 2007. *Pengantar Teknologi Informasi*. Jakarta: Salemba Infotek, halaman 457.

Ada beberapa faktor yang mendorong semakin maraknya aksi *cyber terrorism*. Faktor-faktor tersebut apabila dirinci antara lain: adanya ketergantungan pada komputer, kelemahan sistem yang dapat dieksploitasi, nilai informasi yang semakin berharga, bertambahnya jumlah operator komputer, banyaknya jumlah *software* yang tersedia sehingga memudahkan kegiatan *hacking/cracking*, mengabaikan sikap waspada pada penggunaan konfigurasi keamanan jaringan, teknologi pengamanan selalu tertinggal dibandingkan teknologi informasi, tidak ada atau kurang diterapkannya kebijakan sekuriti intern dari setiap organisasi, dan belum adanya manajemen aksi preventif yang proaktif, adanya penerapan *e-government* bagi pemerintah Indonesia.³⁸

1. Adanya ketergantungan pada komputer

Hukum pada dasarnya merupakan batasan bagi masyarakat dalam bertindak laku terhadap pelanggaran dan untuk itu diperlukan sanksi dengan daya paksa otoritas tertinggi dalam kedaulatan suatu negara. Hukum diperlukan untuk menciptakan ketertiban dalam masyarakat dan memberikan keadilan. Ketertiban dan keadilan itu diperuntukan bagi individu maupun kolektif. Kemajuan teknologi yang berkembang dalam dunia modern saat ini adalah kemajuan yang ditandai setiap orang menggenggam dunia dengan sentuhan jari dalam perangkat teknologi, dan setiap orang melakukan interaksi sosialnya dengan seluruh giat dari jarak jauh dimulai dari ruang maya.

2. Kelemahan Sistem Yang Dapat Dieksploitasi

³⁸ Dikdik M Arief Mansur dan Elisatris Gultom. *Op. Cit.*, halaman 58.

Kelemahan sistem yang dapat dieksploitasi disini adalah, kurangnya pengamanan sistem di negara Indonesia ini. Dalam kurangnya pengamanan teknologi yang ada di negara ini masih kurang canggih dan modern dibandingkan dari negara-negara lainnya. Sehingga sistem kita masih mudah untuk di *hack* atau dimasukkan oleh sistem lain yang ingin bertindak kejahatan. Dalam hal ini sumber daya manusia yang kurang untuk membangun sistem yang kuat supaya tidak dengan mudah untuk dieksploitasi.

3. Nilai Informasi Yang Semakin Berharga

Informasi sangat dibutuhkan oleh siapapun baik untuk antar masyarakat apalagi untuk negara, dalam tindak pidana *cyber terrorism* ini, pelaku yang melakukan tindak pidana *cyber terrorism* akan mencari tahu informasi-informasi apa saja yang akan dibutuhkan pelaku untuk melancarkan tugas yang telah mereka susun sehingga dalam pemberitahuan informasi yang penting sangat diperlukan sifat kehati-hatian untuk tetap menjaga dan tidak terjadinya tindak pidana *cyber terrorism*.

4. Bertambahnya Jumlah Operator Komputer

Perkembangan teknologi dimasa ini semakin hari semakin maju sehingga operator komputer sangat banyak, bahkan sudah sampai ke pelosok desa, dalam hal ini pelaku tindak pidana *cyber terrorism* dengan mudah melakukan aksinya dengan menggunakan komputer yang tersedia dimana-mana.

5. Banyaknya Jumlah *Software* Yang Tersedia Sehingga Memudahkan Kegiatan *hacking/cracking*

Jumlah *software* yang tersedia sangat mudah dan melancarkan aksi *hacking/cracking* si pelaku *cyber terrorism* dalam melakukan aksinya. Kegiatan ini juga sangat mudah dipelajari sehingga siapapun dapat melakukannya. Seharusnya pemerintah dalam hal ini harus memperketat pengawasan demi meminimalisir dan mencegah terjadinya tindak pidana *cyber terrorism*.

6. Mengabaikan Sikap Waspada Pada Penggunaan Konfigurasi Keamanan Jaringan

Pemerintah kurang peduli akan keamanan jaringan yang ada di negara ini, sehingga para pelaku *cyber terrorism* sangat mudah untuk melakukan *hacking/cracker* kepada sistem jaringan yang tersedie. Kurangnya sikap waspada dan kehati-hatian salah satu terjadinya tindak pidana *cyber terrorism* tersebut.

Mengapa gerak di ruang dunia maya itu harus dibatasi dengan perangkat hukum oleh karena kehidupan nyata itu berpindah ke ruang maya dengan segala aspek negatif yang terjadi dan menjadi persoalan hukum. *Cyberspace* merupakan dunia virtual yang dibentuk dari hasil penyatuan antara manusia dan teknologi, yaitu dari perkembangan teknologi informasi dan komunikasi (*Information and communication technology*). Teknologi Informasi dan komunikasi merupakan gabungan dari teknologi komputer, telekomunikasi serta jaringan komputer dan telekomunikasi. Di dalam dunia *cyberspace* bersifat *borderless* itu setiap orang datang dari mana saja dan kapan saja serta dapat memasuki ruang yang teramat luas untuk saling berkomunikasi tanpa perlu berada secara fisik di dalam ruang tempat mereka berkomunikasi.

Di ruang maya *cyberspace* itu sebagai dunia baru dalam kehidupan manusia modern terdapat makna hak asasi manusia. Dunia *cyber* tiap manusia memiliki eksistensi diri yaitu memiliki kebebasan mendasar sebagai salah satu hak bagi setiap orang untuk tidak menggunakan identitas asli, meski di Indonesia kulturnya berbeda dengan jelas menggunakan identitas diri asli. Semakin berkembang dunia maya maka semakin berkembang juga ideologi kebebasan dalam dunia *cyber*.

Akan tetapi regulasi dalam dunia nyata untuk menarik permasalahan hukum dari ruang maya yang terjadi tetap diperlukan, hingga dibutuhkan perangkat hukum untuk menyelesaikan perkara hukum yang terjadi di ruang maya (*cyberspace*) itu. Tidak hanya pemenuhan dalam struktur hukum saja sebagai penangkal kejahatan yang timbul akibat dari kegiatan *cyber* ini namun yang yang terpenting lagi adalah budaya hukum masyarakat dalam merespon aturan-aturan hukum yang diberlakukan.

7. Teknologi Pengamanan Selalu Tertinggal Dibandingkan Teknologi Informasi

Meluasnya ancaman terorisme di berbagai negara tidak terlepas dari pengaruh kemajuan teknologi, terutama internet, yang kemudian akibat penyalahgunaan jaringan internet, yang dikenal dengan *cyber crime*. Penyalahgunaan internet untuk aksi terorisme lebih dikenal dengan *cyber terrorism*. Di sini internet dimanfaatkan oleh teroris untuk melancarkan aksi-aksinya. Pelaku-pelaku *cyber crime/cyber terrorism* secara umum adalah orang-orang yang mempunyai keunggulan kemampuan keilmuan dan teknologi.

Siapapun orangnya yang mempunyai kemampuan menggunakan internet bisa terjebak menjadi korban kejahatan ini. Namun sebaliknya, seseorang juga dapat dengan mudah menjadi penjahat-penjahat akibat terkondisikan secara terus-menerus atau dipaksa secara psikologis dan budaya untuk mengikuti serta berkiblat kepada pengaruh kriminalitas dan disnormatifitas yang dipenetrasikan masyarakat global.

Sehingga perlu adanya pembaharuan-pembaharuan dalam substansi hukum berbasis teknologi yang ada sekarang agar setiap aktifitas yang merugikan dapat diantisipasi dan ditangani secara menyeluruh. Namun kenyataannya, perkembangan teknologi pengamanan jauh tertinggal dengan perkembangan teknologi informasi.

8. Tidak Ada Atau Kurang Diterapkannya Kebijakan Sekuriti Intern Dari Setiap Organisasi

Pengamanan sangat perlu dalam menjaga pertahanan dan keamanan negara. Dalam hal terjadinya tindak pidana *cyber terrorism* ini adalah salah satunya kurang pengamanan. Di Indonesia sering kali terjadi sikap lalai dalam melakukan sesuatu, apabila sudah terjadi kesalahan dan musibah baru dilakukan pengamanan. Seharusnya disini harus dilakukan sikap kehati-hatisn demi menjaga pertahanan dan keamanan negara.

9. Belum Adanya Manajemen Aksi Preventif Yang Proaktif

Aksi prenentif sangat bagus dilakukan demi mencegah terjainya tindak pidana *cyber terrorism* yang dapat mengancam negara dan masyarakatnya. Kurangnya aksi preventif ini yang menimbulkan terjadinya tindak pidana *cyber*

terrorism tersebut. perlu kiranya pemerintah melakukan aksi prefentif yang proaktif demi menjaga pertahanan dan keamanan negara dan masyarakat yang ada didalamnya.

10. Adanya Penerapan *e-government* Bagi Pemerintah Indonesia

Berkemangnya infrastruktur vital berbasis komputerisasi seperti sistem perbankan, *e-commerce*, *e-government* dan lain-lain maka potensi kejahatan terorisme dengan kemanfaatan teknologi informasi sangat rentan terjadi dalam ruang maya (*cyberspace*). Contoh nyata ditemukannya laptop yang digunakan salah satu tokoh peledakan bom bali imam samudera yang disita penyidik, dan diketahui adanya hubungan yang kuat antara aksi terorisme dengan tindak pidana berbasis teknologi informasi, bahwa internet dijadikan sarana komunikasi, propaganda, serta *cardign* untuk memperoleh dana bagi pembiayaan aksi teror.

Kemajuan teknologi informasi dan telekomunikasi memicu semakin berkembangnya bentuk-bentuk kejahatan terorisme di ruang maya. Kemajuan seni dan ilmu pengetahuan tidak menunjukkan moralitas manusia. Masyarakat itu sendirilah yang melahirkan suatu kejahatan. Semakin tinggi tingkat intelektualitas suatu masyarakat, maka semakin canggih pula kejahatan yang mungkin terjadi dalam masyarakat tersebut.

C. Kendala Dalam Pelaksanaan Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme

Masalah-masalah *cyber terrorism* selalu menjadi masalah yang menarik karena beberapa alasan, antara lain karena permasalahan tersebut masih tergolong baru, berkaitan dengan teknologi yang hanya sebagian orang mampu

melakukannya, terbatasnya jangkauan hukum untuk mengantisipasi dan lain sebagainya. Di Indonesia penanganan permasalahan ini sudah semakin intensif sejak maraknya kejadian pemboman ditempat-tempat umum sehingga permasalahan ini terus berimbas pada kepercayaan terhadap dunia usaha di Indonesia.

Salah satu bentuk tindak kejahatan yang menjadi prioritas untuk ditindaklanjuti adalah tindak pidana kejahatan terorisme dunia maya (*cyber terrorism*). Adapun beberapa kendala yang disering dihadapi dalam pelaksanaan Undang-undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme yang berkaitan dengan dunia maya adalah kendala intern dan kendala ekstern.

1. Kendala Intern

Untuk dapat berjalannya sistem hukum, maka diperlukan adanya keterpaduan antara substansi hukum (*legal substance*), struktur hukum (*legal structure*), dan budaya hukum (*legal culture*). Yang dimaksud dengan substansi hukum adalah aturan, norma, dan pola perilaku manusia yang nyata dalam sistem hukum, dapat juga yang berupa produk yang dihasilkan oleh orang yang berada dalam sistem tersebut, mencakup keputusan yang mereka keluarkan, aturan baru yang mereka susun, juga mencakup *living law* (hukum yang hidup diwilayah itu), dan bukan hanya aturan yang ada dalam undang-undang (*law in the book*). Pembahasan di atas, yang dimaksud dengan struktur hukum adalah para pelaku yang ada didalam instansi penegak hukum (kepolisian, kejaksaan, pengadilan) yang dapat disimpulkan bahwa struktur hukum itu adalah mesin penggerak

instansi penegak hukum. Yang dimaksud dengan budaya hukum adalah pandangan, reaksi manusia terhadap hukum dan sistem hukum yang berlaku disekitarnya, yang didalamnya terdapat kepercayaan, nilai, pemikiran serta harapan. Dan dapat disimpulkan bahwa sebenarnya budaya hukum itu adalah suasana pemikiran sosial dan kekuatan sosial yang menentukan bagaimana hukum itu digunakan.

Kendala intern yaitu hal yang berasal dari undang-undang itu sendiri. Adapun hal intern yang menjadi kendala dalam pelaksanaan Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme adalah masih terdapatnya beberapa kelemahan pasal-pasal dalam undang-undang tersebut, misalnya pada Pasal 26. Selama ini, polisi terkesan dominan dalam pemberantasan terorisme. Padahal, polisi masih terikat KUHAP, sehingga sulit menjangkau teroris. Pasal 26 Undang-undang Nomor 15 Tahun 2003 menunjukkan bahwa polisi harus memenuhi syarat-syarat formalitas untuk mengungkap kejahatan terorisme, seperti harus ada dua alat bukti sebagai bukti permulaan yang cukup.

Pasal 26, menyatakan:

- (1) Untuk memperoleh bukti permulaan yang cukup, penyidik dapat menggunakan setiap laporan intelijen.
- (2) Penetapan bahwa sudah dapat atau diperoleh bukti permulaan yang cukup sebagaimana dimaksud dalam ayat (1) harus dilakukan proses pemeriksaan oleh Ketua atau Wakil Ketua Pengadilan Negeri.
- (3) Proses pemeriksaan sebagaimana dimaksud dalam ayat (2) dilaksanakan secara tertutup dalam waktu paling lama 3 (tiga) hari.
- (4) Jika dalam pemeriksaan sebagaimana dimaksud dalam ayat (2) ditetapkan adanya bukti permulaan yang cukup, maka Ketua Pengadilan Negeri segera memerintahkan dilaksanakan penyidikan.

Kelemahan undang-undang ini mengharuskan polisi untuk mendapat perintah Pengadilan Negeri untuk melakukan penyidikan. Waktu yang dibutuhkan itu tiga hari. Lalu penyidikannya harus mendapatkan perintah terlebih dahulu dari pengadilan negeri setempat sehingga memang sangat menyita waktu. Jika mengacu pada Undang-undang terorisme, sebenarnya tindakan polisi menembak mati teroris melanggar Undang-undang terorisme. Seorang terduga teroris juga harus mendapatkan haknya, seperti didampingi pengacara. Jika hal ini terjadi tentunya polisi telah melanggar Undang-undang itu.

Ketika Polisi dengan KUHAP-nya tidak dapat menjangkau pencegahan terorisme, maka harus ada instrumen negara yang harus mengisi kekurangan atau kelemahan itu. Teroris dalam menyiapkan aksinya sering melakukan pergerakan intelijen antara lain dalam perekrutan, penggalangan, perencanaan dan baru aksi. Semuanya berada di bawah layar sehingga kepolisian sulit membuktikannya. Tindak pidana terorisme itu memiliki spektrum sangat luas kemudian sifat dan karakternya juga berbeda dari tindak pidana lainnya. Sangat jelas dalam penanganan tindak pidana terorisme tidak hanya penegakan hukum oleh polisi yang dibutuhkan, namun justru lebih kental pencegahannya yaitu bentuk deteksi dini dan cegah dini. Undang-undang Nomor 15 Tahun 2003 juga belum secara komprehensif mengatur ketentuan delik tindak pidana, misalnya delik percobaan. Perlu redefinisi istilah terorisme, karena istilah Terorisme dan teroris sekarang ini memiliki arti politis sehingga menjadi kendala dalam pelaksanaannya.

2. Kendala Ekstern

Kendala ekstern yaitu kendala yang dialami dari luar undang-undang itu sendiri. Dalam pelaksanaan UU No. 15 Tahun 2003 terdapat beberapa kendala yaitu: baik dari kurangnya sarana yang memadai bagi polisi dalam menjalankan tugasnya, keterbatasan pengetahuan/ tenaga ahli, dan kurangnya kepercayaan masyarakat terhadap Polisi.

- a) Kurangnya sarana dan prasarana yang memadai bagi polisi dalam melaksanakan tugasnya.

Kurangnya sarana yang memadai dalam pemberantasan tindak pidana *cyber terrorism* dapat menjadi penghambat dalam menanggulangi kejahatan tersebut. Disiapkannya UU tanpa dibarengi dengan persiapan sarana dan prasarana menjadikan produk UU tersebut tidak bisa dijalan sepeserti yang diharapkan. Indonesia termasuk kedalam negara besar yang terdiri dari beberapa wilayah dengan jumlah pengguna layanan internet yang sangat besar pula sehingga para pelaku *cyber terrorism* sangat leluasa melakukan kejahatan. Dengan demikian, kepolisian membutuhkan alat yang canggih dalam menjangkau semua wilayah.

- b) Keterbatasan pengetahuan/tenaga ahli

Keterbatasan pengetahuan akan IT yang terdapat merupakan salah-satu kendala yang sedang perbaiki oleh pihak pemerintah. Untuk beberapa kasus-kasus kejahatan *cyber terrorism* yang besar biasanya dilakukan oleh orang-orang memiliki pengetahuan yang tinggi terhadap penggunaan Teknologi Informasi. Seringkali pelaku teror melalui internet sengaja secara terang-terangan melakukan kejahatan mereka karena mereka sudah ahli dalam teknologi dan dalam sekejap pula dengan pengetahuan IT yang sudah mumpuni mereka bersembunyi dengan

menghilangkan data-data terkait kejahatan mereka. Namun, pihak kepolisian sendiri masih sangat sulit menggunakan alat bantu yang ada karena kurangnya pengetahuan mereka dalam IT. Masuknya UU terorisme tidak disertai dengan persiapan perkembangan ilmu pengetahuan dan teknologi sehingga UU ini tidak bisa dilaksanakan sepenuhnya.

c) Kurangnya kepercayaan masyarakat terhadap Polisi

Kurangnya kepercayaan masyarakat terhadap penegak hukum sekarang ini bukan menjadi suatu hal yang asing lagi, hilangnya rasa kepercayaan terhadap instansi Kepolisian dalam perannya menanggulangi tindak pidana *cyber terrorism* merupakan efek dari respon masyarakat terhadap penegakkan hukum di negeri ini. Problematika penegakkan hukum ini dipengaruhi karena lemahnya mentalitas para penegak hukum diantaranya lemahnya pemahaman agama, ekonomi, dan tugas-tugas yang menjadi kewajiban mereka sebagai penegak hukum. Hal inilah yang menjadi kendala dalam pelaksanaan Undang-undang Nomor 15 Tahun 2003.

BAB IV

KESIMPULAN DAN SARAN

A. Kesimpulan

1. Kelemahan Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme dalam upaya mencegah dan menanggulangi aktivitas cyberterrorism yaitu tidak mencakup propaganda dan dukungan terhadap terorisme. Kelemahan tersebut masih dapat ditutupi oleh ketentuan- ketentuan dalam Pasal 155 ayat (1), 156, 157 ayat (1), 160 KUHP dan Pasal 28 Ayat (2) j.o Pasal 45 Ayat (2) Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun, kebijakan kriminalisasi dalam KUHP dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik hanya mencakup penyebar, bukan pembuat informasi propaganda.
2. Ada beberapa faktor yang mendorong semakin maraknya aksi *cyber terrorism*. Faktor-faktor tersebut apabila dirinci antara lain: adanya ketergantungan pada komputer, kelemahan sistem yang dapat diekplotasi, nilai informasi yang semakin berharga, bertambahnya jumlah operator komputer, banyaknya jumlah *software* yang tersedia sehingga memudahkan kegiatan *hacking/cracking*, mengabaikan sikap waspada pada penggunaan konfigurasi keamanan jaringan, teknologi pengamanan selalu tertinggal dibandingkan teknologi informasi, tidak ada atau kurang diterapkannya kebijakan sekuriti intern dari setiap

organisasi, dan belum adanya manajemen aksi preventif yang proaktif, adanya penerapan *e-government* bagi pemerintah Indonesia.

3. Adapun beberapa kendala yang disering dihadapi dalam pelaksanaan Undang-undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme yang berkaitan dengan dunia maya adalah kendala intern meliputi adanya aturan pasal yang lemah seperti pada Pasal 26 dan kendala ekstern yaitu yang berasal dari luar undang-undang itu sendiri meliputi baik dari kurangnya sarana yang memadai bagi polisi dalam menjalankan tugasnya, keterbatasan pengetahuan/ tenaga ahli, dan kurangnya kepercayaan masyarakat terhadap Polisi.

B. Saran

1. Banyaknya terjadi kasus kejahatan internet (*cyber crime*) khususnya dalam kejahatan *cyber terrorism* yang menimbulkan banyaknya korban yang mengalami kerugian baik materil mau moril yang disebabkan oleh banyak faktor seharusnya dapat menyadarkan untuk lebih berhati-hati dan bijak dalam penggunaan penggunaan layanan internet. Polisi sebagai aparat yang dipercayakan oleh negara untuk menjalankan fungsi dan wewenangnya dalam penegakkan hukum, pemeliharaan keamanan dan ketertiban umum, serta perlindungan, pengayoman, dan pelayanan masyarakat berkewajiban untuk mencegah dan menanggulangi tindak kejahatan terorisme diinternet secara lebih aktif lagi. Dalam penanganan, dan penanggulangan tindak kejahatan

internet (*cyber crime*) tentunya harus bekerja sesuai dengan Undang-undang yang berlaku dengan tetap menjunjung tinggi hukum dan HAM.

2. Bahwa pemerintah Republik Indonesia sebaiknya dibuat peraturan perundang-undangan yang khusus mengenai tindak pidana cyber terrorism atau melakukan perubahan terhadap Undang-undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme mengingat bahwa tidak semua pasal dapat digabungkan Karena apabila di lihat sekarang tindak pidana ini sangat potensial terjadi di Indonesia karena kemajuan teknologi dalam kehidupan masyarakat.
3. Bahwa perlu adanya sikap antisipatif dari pemerintah Indonesia dengan merevisi undang-undang, memperketat pertahanan system teknologi, system komunikasi dan perlu membentuk lembaga khusus yang memegang kendali seluruh jaringan teknologi dan komunikasi di Indonesia agar semua bentuk kemungkinan kejahatan melalui teknologi informasi dapat di cegah sehingga dapat melindungi bangsa Indonesia dari kehancuran.

DAFTAR PUSTAKA

A. Buku

- Abdul Manan. 2006. *Aspek-aspek Pengubah Hukum*. Jakarta: Kencana.
- Abdul Wahid, Mohammad Labib. 2010. *Kejahatan Mayantara (cyber crime)*. Bandung: Refika Aditama.
- Adami Chazawi. 2002. *Pelajaran Hukum Pidana Bagian I*. Jakarta: Rajawali pers.
- Ali Murthado dan Mustafa Kamal Rokan. 2012. *Metodologi Penelitian Hukum Suatu Pemikiran dan Penerapan*. Medan: Wal Ashri Publishing.
- Aji supriyanto. 2007. *Pengantar Teknologi Informasi*. Jakarta: Salemba Infotek.
- Barda Nawawi Arief, 2007. *Tindak pidana mayantara: perkembangan kajian cyber crime di Indonesia*. Jakarta: Raja Grafindo Persada.
- Beni Ahmad Saebani. 2009. *Metode Penelitian Hukum*. Bandung: Pustaka Setia.
- Budi suharianto. 2013. *Tindak Pidana Teknologi Informasi (cybercrime)*. Jakarta: PT Raja Grafindo.
- Dikdik M Arief Mansur dan Elisatris Gultom. 2009. *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama.
- Dyah Ochtorina Susanti dan A'an Efendi. 2014. *Penelitian Hukum (Legal Research)*. Jakarta: Sinar Grafika.
- E.Y Kanter dan S.R. Sianturi. 2012. *Asas-Asas Hukum Pidana Di Indonesia Dan Penerapannya*. Jakarta: Storia Grafika.
- Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. 2014. *Pedoman Penulisan Skripsi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara*. Medan: Fakultas Hukum Universitas Muhammadiyah Sumatera Utara.
- Josua Sitompul. 2012. *Cyberspace, cybercrimers, cyberlaw*. Jakarta: Tatanusa.
- Mahrus Ali. 2015. *Asas-Asas Hukum Pidana Korporasi*. Jakarta: Raja Grafindo.
- Mardenis. 2013. *Pemberantasan Terorisme: Politik Internasional dan Politik Hukum Nasional Indonesia*. Jakarta: Rajawali pers.
- Petrus Reinhard Golose. 2009. *Deradikalisasi Terorisme: Humanis, Soul Approach dan Menyentuh Akar Rumput*. Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian.

P.A.F Lamintang. 1996. *Dasar-Dasar Hukum Pidana Indonesia*. Bandung: Citra Aditya Bakti.

Sinta Dewi Rosadi. 2015. *Cyber Law (aspek data privasi menurut hukum internasional, regional, dan nasional)*. Bandung: Refika Aditama.

Suharyo. 2012. *Penelitian Hukum Tentang Penerapan bantuan Timbal Balik Dalam Masalah Pidana Terhadap Kasus-kasus Cybercrime*. Cililitan: BPHN Kemenkumham RI.

B. Peraturan Perundang-undangan

Undang-undang Dasar Negara Republik Indonesia Tahun 1945

Undang-undang Nomor 1 Tahun 1946 Tentang Peraturan Hukum Pidana

Undang-undang Nomor 8 Tahun 1981 Tentang Peraturan Hukum Acara Pidana

Undang-undang Nomor 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

C. Internet

Barda Nawawi Arif, “Pengertian Pelaku”, melalui <http://www.pengertianpelakudalamhukumpidana.com>, diakses Sabtu, 13 Agustus 2016.

Eptik Bsikel, “Pengertian Cyber Terrorism”, melalui <http://eptikbsikel9.blogspot.co.id/2015/04/pengertian-cyber-terrorism.html>, diakses Kamis, 18 Agustus 2016.

Word Press, “Cyber Crime Dihubungkan Dengan Tindak Pidana”, melalui <https://konsultasihukum2.wordpress.com/2010/08/29/cyber-crime-dihubungkan-dengan-tindak-pidana-terorisme/> , diakses Sabtu , 27 Agustus 2016.



Keagamaan, Cerdas dan Tanggungjawab

MAJELIS PENDIDIKAN TINGGI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM

Jalan Kapten Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6623301 Fax. (061) 6625474
Website : <http://www.umsu.ac.id> E-mail : rektor@umsu.ac.id
Bankir : Bank Syariah Mandiri, Bank Mandiri, Bank BNI 1946, Bank Sumut.

KARTU BIMBINGAN
SKRIPSI MAHASISWA

Nama Mahasiswa : M. HABIBIE GINTING
NPM : 1206200441
Prodi/Bagian : ILMU HUKUM/HUKUM PIDANA
Judul Skripsi : TINJAUAN YURIDIS TERHADAP PELAKU *CYBER TERRORISM*
MENURUT UNDANG-UNDANG NOMOR 15 TAHUN 2003
TENTANG PEMBERANTASAN TINDAK PIDANA TERORISME

Pembimbing I : ASLIANI HARAHAHAP, S.H., M.H
Pembimbing II : RACHMAD ABDUH, S.H., M.H

TANGGAL	MATERI BIMBINGAN	KONS. LANJUTAN	PARAF
29/09-2016	Penjelasan Skripsi.		
2/10 2016	Metode Penelitian		
14/10 2016			
19/10 2016	Sec. Ke P. 1		
10/10-2016	Penyusunan skripsi		
19/10-2016	Perhatikan pembina bab I, II & III		
22/10-2016	See untuk diperbanyak dan diujikan		

Diketahui Dekan

IDA HANIFAH, S.H., M.H

Pembimbing I

ASLIANI HARAHAHAP, S.H., M.H

Pembimbing II

RACHMAD ABDUH, S.H., M.H