BAB II

TINJAUAN PUSTAKA MENGENAI KEBIJAKAN HUKUM PIDANA *CYBER TERRORISM* DI INDONESIA

A. Tinjauan Tentang Kebijakan Hukum Pidana

1. Pengertian Kebijakan Hukum Pidana

Teori kebijakan hukum pidana biasa juga dikenal sebagai politik hukum pidana. Kebijakan hukum pidana (*criminal law policy*) atau kebijakan penal (*penal policy*) dapat diartikan sebagai usaha yang rasional untuk menanggulangi kejahatan (politik kriminal) dengan menggunakan sarana hukum pidana yaitu dari kebijakan atau politik hukum pidana (*strafrechtspolitiek*).(Kenedi, 2017, hal. 5) Melaksanakan kebijakan dengan usaha guna membentuk peraturan hukum yang berkualitas pada dasarnya merupakan salah satu tujuan penanggulangan kejahatan. Ini berarti bahwa politik kriminal menjadi induk dari pelaksanaan kebijakan atau politik hukum pidana. Dinilai dari sisi politik kriminal, politik hukum pidana memiliki makna yang sama dengan kebijakan yang dibuat guna menanggulangi tindak kejahatan dengan menggunakan hukum pidana.

Upaya penanggulangan kejahatan dapat dibedakan menjadi 2 (dua) yaitu melalui jalur *"penal"* (hukum pidana) dan melalui jalur *"non-penal"* (diluar hukum pidana). Penerapan hukum pidana tidak terlepas dari adanya suatu peraturan undang-undang pidana. (Hattu, 2014, hal. 48) Menurut Sudarto, dengan upaya untuk mencapai status pidana yang dengan keadaan, situasi waktu dan masa yang akan datang, masalahnya adalah implementasi kebijakan hukum pidana. (Alfauzi,

2016, hal. 29) Upaya penanggulangan kejahatan melalu jalur *penal* menitikberatkan sifat *repressive* yaitu penindasan/pemberantasan setelah kejahatan terjadi.(Hattu, 2014, hal. 49) Upaya pencegahan dan penanggulangan kejahatan melalui sarana penal merupakan suatu usaha yang memuat suatu peraturan yang mencantumkan pemidanaan.(Rotua Pardede, 2019, hal. 28) Upaya penanggulangan kejahatan dikenal dengan berbagai istilah, antara lain kebijakan penal (*penal policy),* kebijakam pidana (*criminal policy),* atau politik hukum pidana (*strafrechtspolitiek)* adalah suatu usaha untuk menanggulangi tindak kejahatan melalui penegakan hukum pidana yang rasional yaitu memenuhi rasa keadilan dan daya guna. Dalam rangka menanggulangi kejahatan terhadap berbagai sarana sebagai reaksi yang dapat diberikan kepada pelaku kejahatan, berupa sarana pidana maupun non hukum pidana, yang dapat diintegrasikan satu dengan yang lainnya.(Kenedi, 2017, hal. 26)

Pembuatan peraturan pidana atau perumusan tindak pidana baru haruslah berorientasi pada perbaikan pelaku maupun perlindungan korban. Hukum pidana bukan lagi suatu alat untuk membalas dendam atau memberikan hukum yang seberat-beratnya terhadap pelaku. Pembaharuan hukum haruslah dilakukan dengan pendekatan kebijakan, karena memang pada hakikatnya ia hanya merupakan bagian dari suatu langkah kebijakan atau *policy*. Di dalam setiap kebijakan *(policy)* terkandung pula pertimbangan nilai. Penggunaan hukum pidana sebenarnya juga bukan merupakan suatu keharusan, karena pada hakekatnya masalah pengendalian atau penanggulangan kejahatan dengan menggunakan hukum pidana, bukan hanya merupakan problem sosial, tetapi juga merupakan masalah kebijakan.(Dwi Laksana, 2021, hal. 3)

Kebijakan hukum yang dilaksanakan dengan sarana *penal* merupakan rangkaian dari tiga tahap.

a.Tahap kebijakan legislatif/*formulatif,*

b.Tahap kebijakan yudikatif/*aplikatif,*

c.Tahap kebijakan eksekutif/*administratif.*

Pada tahap pengembangan pencegahan kejahatan (tahapan formulasi), ini memberikan tanggung jawab legislatif untuk menentukan bentuk-bentuk tindakan yang dapat dituntut dan diatur oleh sistem peradilan pidana terpadu dan terpadu (kebijakan legislatif).(Kenedi, 2017, hal. 7) Dari perspektif kebijakan hukum, melaksanakan politik hukum pidana atau kebijakan peradilan pidana memiliki dua implikasi. Pertama, upaya untuk menerapkan peraturan yang tepat (di masa depan) sesuai dengan situasi dan keadaan umum. Kedua, kebijakan nasional melalui badan-badan yang terakreditasi untuk mewakili apa yang terkandung dalam masyarakat dan menetapkan peraturan-peraturan yang diinginkan yang digunakan untuk mencapai apa yang diinginkan. Menegakkan politik hukum berarti mengadakan pemilihan umum untuk hasil terbaik dari hukum pidana dalam hal memenuhi tuntutan keadilan dan efisiensi. Pelaksanaan politik hukum juga dapat berarti upaya untuk melaksanakan peraturan perundang-undangan pidana dalam setiap situasi dan untuk masa yang akan datang.(Amrani, 2019, hal. 4)

Usaha dan kebijakan untuk membuat peraturan hukum pidana yang baik pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan. Jadi kebijakan atau politik hukum pidana juga merupakan bagian dari politik kriminal *(criminal policy).* Sebagai bagian dari politik kriminal, politik hukum pidana

identik dengan pengertian kebijakan penanggulangan kejahatan dengan hukum pidana.(Amrani, 2019, hal. 5) Dilihat dari politik hukum, maka melaksanakan politik hukum pidana mempunyai dua arti. Pertama, usaha untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi yang ada pada suatu saat (termasuk kedepannya). Kedua, kebijakan dari negara melalui badan yang berwenang untuk menetapkan peraturan-peraturan yang dikehendaki yang diperkirakan dapat digunakan untuk mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang dicita-citakan. Melaksanakan kebijakan hukum pidana berarti mengadakan pemilihan untuk mencapai hasil perundangan pidana yang paling baik dalam arti memenuhi syarat keadilan dan daya guna. Disamping itu, melaksanakan kebijakan hukum pidana dapat pula berarti usaha mewujudkan peraturan perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa-masa yang akan datang. (Amrani, 2019, hal. 6)

Menurut March Ancel, *penal policy* atau kebijakan hukum pidana merupakan suatu ilmu sekaligus seni yang pada akhirnya mempunyai tujuan praktis untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik dan untuk memberi pedoman tidak hanya kepada pembuat undang-undang, tetapi juga kepada pengadilan yang menerapkan undang- undang dan juga kepada para penyelenggara atau pelaksana urusan pengadilan.(Yuspin et al., 2020, hal. 11) Politik kriminal merupakan bagian dari politik penegakan hukum dalam arti luas. Semuanya merupakan bagian dari politik sosial, yakni usaha dari masyarakat atau negara untuk meningkatkan kesejahteraan warganya.

2. Pengertian Hukum Pidana dan Sanksi Pidana

Di Indonesia, kejahatan *cyber terrorism* tidak diatur dalam KUHP atau peraturan perundang-undangan tentang terorisme, khususnya Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Perpu Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-undang jo. Penetapan Perpu No.1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme serta Undang- undang RI No. 9 Tahun 2013 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme. Hal ini menciptakan adanya kekosongan hukum untuk mengelola kejahatan *cyber terrorism*, menurut analisis hukum yang berlaku di Indonesia.

Pengaturan *Cyber Terrorism* di dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik diundangkan pada tanggal 21 April 2008 yang mana undang-undang ini bukanlah undang-undang tindak pidana khusus dikarenakan tidak semata-mata memuat ketentuan hukum pidana secara keseluruhan namun memuat pengaturan tentang pengelolaan informasi dan transaksi elektronik di tingkat nasional.(Josianto Adam, 2014, hal. 164)

Ciri utama terorisme siber adalah tindakan terorisme terhadap sistem komputer, jaringan dan/atau pangkalan, dan informasi yang tersimpan di komputer. Tindakan yang termasuk dalam kategori ini memiliki format sebagai berikut:

a. *Unauthorized access to computer system and service*, yaitu kejahatan menggunakan system komputer melalui jaringan secara tidak benar dan tanpa ijin dari pemilik,

b. *Denial of service attack* (DoS), yakni menyerang dengan cara memenuhi jaringan dengan permohonan dalam hitungan detik untuk mendapatkan layanan data sehingga mengakibatkan jaringan bekerja terlalu keras, atau mati, atau melambatnya kinerja jaringan,

c. *Cyber sabotage and extortion*, yaitu kejahatan yang dilakukan dengan menggangu, merusak, atau menghancurkan suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet,

d. *Viruses*, yakni kejahatan yang dilakukan dengan menyebarkan perangkat lunak seperti program, script, atau macro yang telah dirancang untuk menginfeksi, menghancurkan, memodifikasi, dan menimbulkan masalah terhadap komputer atau program komputer,

e. *Physical attacks*, yakni penyerangan fisik yang dilakukan terhadap sistem komputer atau jaringan komputer, dengan cara-cara pembakaran, pencabutan salah satu *device* komputer atau jaringan yang menyebabkan lumpuhnya sistem komputer.

Beberapa dari lima tindakan di atas, jika diselidiki, adalah beberapa tindakan yang dilarang oleh undang-undang ITE dan dirinci di bawah ini:

a. Pasal 30 UU ITE mengatur tentang tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun. Konstruksi perbuatan dalam rumusan pasal ini menjelaskan bahwa tindakan tidak sah/illegal yang dilakukan oleh seseorang terhadap sistem elektronik milik orang lain dengan tujuan untuk memproleh informasi/dokumen

elektronik dan/atau upaya pembobolan, penerobosan, dan penjebolan yang melanggar dan melampaui sistem pengamanan,

b. Pasal 32 dan Pasal 33 UU ITE yang mengatur tentang perlindungan terhadap suatu informasi dan/atau dokumen elektronik baik milik orang lain atau milik publik yang bersifat rahasia.

Sifat melawan hukum dalam Pasal 30 UU ITE tersebut memiliki dua corak, yakni melawan hukum objektif dan melawan hukum subjektif. Melawan hukum objektif berarti komputer dan/ atau sistem komputer tersebut bukan milik pelaku dan perbuatan mengakses komputer dan/ atau sistem elektronik tersebut tanpa izin pemilik/ tanpa hak. Sama halnya dengan Pasal 30 UU ITE, Pasal 32 UU ITE juga memiliki dua corak sifat melawan hukum. Sifat melawan hukum yang objektif dalam rumusan pasal ini terdapat pada unsur objeknya, bahwa Informasi Elektronik dan/ atau Dokumen Elektronik tersebut milik orang lain. Agar rumusan tersebut memenuhi sifat melawan hukum yang objektif, maka frasa milik orang lain tersebut harus dibuktikan dan dipastikan keberadaannya melalui perbuatan mengubah dan sebagainya tersebut harus tidak ada izin dari pemiliknya. Sedangkan sifat melawan hukum yang subjektifnya terletak pada keadaan batin si pelaku terhadap sifat melawan hukum objektifnya perbuatan. Pelaku mengetahui bahwa perbuatan Yang hendak diperbuatnya adalah yang mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, serta memindahkan,dan menyembunyikan dengan cara apapun suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik sebagai perbuatan yang tercela. Sifat melawan hukum dalam Pasal 33 UU ITE terletak pada akibat perbuatan tersebut, yakni perbuatan

pelaku tersebut akan mengakibatkan terganggunya atau tidak bekerjanya sistem elektronik tersebut sebagaimana mestinya.

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

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

pembentukan para militer melawan hukum, perencanaan, pelaksanaan serangan teroris, persembunyian, dan pendanaan.

Relevansi Pasal 30, Pasal 32, dan Pasal 33 UU ITE dengan perbuatan tindak pidana *cyber terrorism* adalah bentuk perbuatan akses tidak sah atau gangguan terhadap data komputer, informasi/ dokumen elektronik milik orang lain atau milik publik yang dilakukan dengan cara pembobolan, penerobosan, dan penjebolan yang melanggar, melampaui sistem pengamanan, dan sebagainya yang memenuhi unsur cara-cara melakukan teror dalam tindak pidana *cyber terrorism.* Namun, sifat melawan hukum untuk tindak pidana *cyber terrorism* tidak terpenuhi dalam rumusan pasal-pasal UU ITE karena dalam tindak pidana *cyber terrorism* serangan atau ancaman secara melawan hukum tersebut dilakukan terhadap komputer, jaringan komputer, dan data yang tersimpan dalam jaringan tersebut, yang memiliki tujuan untuk mengintimidasi atau memaksa pemerintah atau masyarakat untuk tujuan politik atau sosial tertentu. Sebagaimana terorisme yang dilakukan secara konvensional yang mengakibatkan kerusakan umum atau suasana teror atau rasa takut terhadap orang secara meluas. Sama halnya dengan unsur akibat serangan dalam terorisme konvensional, bahwa suatu tindakan dapat dikategorikan sebagai *cyber terrorism* apabila serangan tersebut menciptakan ketakutan dan mengakibatkan korban pada daerah sekitarnya atau secara meluas, meskipun bukan target utama dari serangan mereka. Hal tersebut menjadikan kekosongan hukum dalam pengaturan UU ITE untuk menanggulangi tindak pidana *cyber terrorism.* Selanjutnya, ciri kedua, yakni *cyber terrorism* sebagai pemanfaatan internet oleh para teroris untuk keperluan organisasi dan media teror kepada pemerintah dan

masyarakat, dapat digali dan dianalisa pengaturannya dalam UU Pemberantasan Tindak Pidana Terorisme, sebagaimana rumusan dalam Pasal 6 UU Pemberantasan Tindak Pidana Terorisme. Pertanggungjawaban pidana merupakan suatu terusan celaan bagi pelaku atas tindak pidana yang telah dilakukannya. Celaan dalam pertanggungjawaban pidana dibagi atas celaan secara objektif dan celaan secara subjektif. Celaan secara objektif berarti pelaku telah melakukan tindak pidana (perbuatan yang dilarang atau melawan hukum dan dapat diberi pidana berdasarkan hukum yang berlaku atau asas legalitas), sedangkan celaan secara subjektif berarti pelaku patut untuk dicela atau diminta pertanggungjawabannya atas tindak pidana yang telah dilakukannya.

Cyber terrorism tidak diatur dalam berbagai Peraturan Perundang-Undangan di Indonesia. *Cyber terrorism* merupakan serangan atau ancaman secara melawan hukum terhadap komputer, jaringan komputer, dan data yang tersimpan dalam jaringan tersebut, yang memiliki tujuan untuk mengintimidasi atau memaksa pemerintah atau masyarakat untuk tujuan politik atau sosial tertentu. Unsur melawan hukum dalam pengertian tersebut dilakukan dengan perbuatan seperti ancaman atau serangan terhadap komputer, jaringan komputer, dan data yang tersimpan dalam jaringan tersebut, sehingga akibat dari melawan hukum ini menciptakan ketakutan atau merusak infrastruktur dan kehidupan manusia. Dalam situasi seperti ini, pelaku tindak pidana *cyber terrorism* dapat dinyatakan bebas dari pidana karena tidak terdapat unsur melawan hukum yang diatur dalam undang-undang melekat pada perbuatannya tersebut. Oleh karena itu, untuk dapat dijatuhi suatu pidana, maka tindak pidana *cyber terrorism* harus dirumuskan secara jelas

dalam Undang-Undang. Unsur melawan hukum dalam tindak pidana *cyber terrorism* tersebut berkaitan dengan asas legalitas karena tidak ada rumusan delik yang mengatur unsur melawan hukum dalam tindak pidana *cyber terrorism*. Sesuai dengan Pasal 1 Ayat (1) KUHP, sebagaimana dikenal sebagai asas legalitas.(Jondong, 2020, hal. 23)

1) . Pengertian Hukum Pidana

Hukum pidana Istilah hukum pidana merupakan terjemahan dari istilah bahasa Belanda "*Strafrecht*", *Straf* berarti pidana, dan *Recht* berarti hukum. Menurut Wirjono Prodjodikoro bahwa istilah hukum pidana itu dipergunakan sejak pendudukan Jepang di Indonesia untuk pengertian *strafrecht* dari bahasa Belanda, dan untuk membedakannya dari istilah hukum perdata untuk pengertian *burgelijkrecht* dari bahasa Belanda. (Dwi Laksana, 2021, hal. 2) Selain itu pengertian hukum pidana juga banyak dikemukakan oleh para sarjana hukum, menurut Soedarto hukum pidana memuat aturan-aturan hukum yang mengikatkan kepada perbuatan-perbuatan yang memenuhi syarat tertentu suatu akibat yang berupa pidana.(Zul Azmi, 2016, hal. 39)

Hukum pidana merupakan salah satu hukum yang berlaku dalam suatu negara yang bertujuan mengatur kehidupan dalam negara, yang bersifat memaksa dan mengikat. Pada dasarnya, kehadiran hukum pidana di tengah masyarakat dimaksudkan untuk memberikan rasa aman kepada individu maupun kelompok dalam masyarakat dalam melaksanakan aktifitas kesehariannya. Rasa aman yang dimaksudkan dalam hal ini adalah perasaan tenang, tanpa ada kekhawatiran akan ancaman ataupun perbuatan yang dapat

merugikan antar individu atau umum dalam kehidupan masyarakat. Kerugian sebagaimana dimaksud tidak hanya terkait kerugian sebagaimana yang kita pahami dalam istilah keperdataan, namun juga mencakup kerugian terhadap jiwa dan raga. Raga dalam hal ini mencakup tubuh yang juga terkait dengan nyawa seseorang, jiwa dalam hal ini mencakup perasaan atau keadaan psikis.(Dwi Laksana, 2021, hal. 2)

2) . Pengertian Sanksi Pidana

Van Kan Hukum mengatakan bahwa hukum pidana tidak mengadakan norma-norma baru dan tidak menimbulkan kewajiban-kewajiban yang dulunya belum ada. Hanya norma-norma yang sudah ada saja yang dipertegas, yaitu dengan mengadakan ancaman pidana dan pemidanaan. Hukum pidana memberikan sanksi yang bengis dan sangat memperkuat berlakunya norma-norma hukum yang telah ada. Tetapi tidak mengadakan norma baru. Hukum pidana sesungguhnya adalah hukum sanksi *(het straf-recht is wezelijk sanctie-recht).*(Zul Azmi, 2016, hal. 36) Sanksi pidana adalah suatu bentuk hukuman yang diberikan terhadap seseorang akibat melakukan suatu pelanggaran hukum. Sanksi pidana diberikan oleh lembaga yang berwenang. Sehingga, kita dapat memahami bahwa pada dasarnya, sanksi pidana merupakan suatu hukuman sebab akibat, sebab merupakan kasusnya dan akibat merupakan hukumnya, orang yang terkena akibat akan memperoleh sanksi baik masuk penjara ataupun terkena hukuman lain dari pihak berwajib. Sanksi Pidana merupakan suatu jenis sanksi yang bersifat nestapa atau derita yang dikenakan terhadap perbuatan atau pelaku perbuatan pidana atau tindak pidana yang dapat

mengganggu atau membahayakan kepentingan hukum. Pada hakikatnya, pembentuk undang-undang pun selalu mengatakan bahwa salah satu usaha dalam penanggulangan kejahatan adalah dengan menggunakan hukum pidana dengan sanksinya berupa pidana.(Suhariyono, 2009, hal. 633)

Menurut Pasal 10 KUHP, sanksi pidana dibedakan dalam sanksi pidana pokok dan sanksi pidana tambahan. Urutan sanksi pidana dalam Pasal 10 dibuat menurut beratnya pidana, di mana yang terberat disebut terlebih dahulu. Dalam penerapan perumusannya pada tiap- tiap pasal dalam Kitab Undang-undang Hukum Pidana digunakan sistem alternatif, dalam arti bila suatu tindak pidana, hakim hanya boleh memilih salah satu saja. Hal ini berbeda dengan sistem kumulatif dimana hakim dapat memilih lebih dari satu jenis pidana.(Kansil, 2014, hal. 33)

Menurut Sudarto dalam bukunya "Kapita Selekta Hukum Pidana" kata pemidanaan sinonim dari penghukuman. Pemidanaan hadir dengan pidana sebagai unsur utamanya memilik tujuan sebagai pembenah pribadi dari seorang yang melakukan suatu tindak pidana, membuat orang tersebut jera dan membuat penjahat tidak dapat mengulangi perbuatannya dengan cara-cara yang lain.(Dwi Laksana, 2021, hal. 2)

Dalam menjatuhkan sebuah pidana pengadilan juga harus memenuhi syarat-syarat yang telah diatur di dalam KUHP atau Undang-Undang. Dewasa ini dalam hukum pidana juga dapat di lihat tedapat sanksi yang merupakan suatu pembalasan dan tidak bersifat sebagai suatu pembalasan melainkan memberikan pendidikan yang sesuai dengan keinginan dari pemerintah sanski

ini disebut sebagai tindakan *(maatregel).* Hal demikian ada, karena adanya anggapan pemidanaan berupa penjatuhan sanksi pidana dalam satu bentuknya yaitu hukuman penjara dapat memenuhi tujuan dari suatu pemidanaan itu sendiri.(Alin, 2017, hal. 23)

Hukum Pidana bertujuan menjatuhkan sanksi "pidana" terhadap siapa saja yang melakukan perbuatan pidana dan melanggar undang-undang hukum pidana adalah sebagai *ultimum remedium* (obat terakhir) dengan tujuan untuk melindungi kepentingan umum atau kepentingan masyarakat.(Zul Azmi, 2016, hal. 49)

Dalam hukum pidana sebagaimana ini diperlukan karena:

1. Sanksi Pidana merupakan sanksi yang dibutuhkan;
2. Sanksi pidana merupakan sarana yang terbaik atau merupakan alat yang terbaik dalam menghadapi kejahatan *(ultimum remedium)*;dan
3. Walaupun di suatu sisi sanksi pidana merupakan penjamin yang terbaik, di sisi lain pengancam utama kebebasan manusia.(Rotua Pardede, 2019, hal. 28)

Penggunaan hukum dalam hukum modern merupakai sarana rekayasa masyarakat *(law as a tool of social engineering)* yang mana dilakukan dengan melibatkan para pembuat hukum dengan merumuskan sanksi sebagai sarana penegakan hukum. Penegakan hukum dilakukan untuk mewujudkan perubahan yang efektif di dalam masyarakat. Penegakan hukum juga dilakukan untuk memenuhi nilai keadilan, terutama bagi korban. Nilai keadilan menjadi sebuah syarat mutlak dalam kehidupan bermasyarakat, berbangsa dan bernegara sesuai

dengan cita hukum Pancasila. Nilai keadilan ini merupakan hal terpenting dalam pembentukan, penerapan dan penegakan hukum. Sampai saat ini formulasi hukum telematika yang terkoneksi melalui internet *(cyberspace)* memang belum mencapai tingkat kemapanan.

Hal ini disebabkan karena bidang ini mengandung unsur-unsur yang kompleks. Mengenai hal tersebut Marco Gercke mengemukakan sebagai berikut: *Introducing cybercrime legislation is not an easy task as there are various areas that require regulation. In addition to substantive criminal law and procedural law, cybercrime legislation may include issues related to international cooperation, electronic evidence and the liability of an Internet Service Provider (ISP). In most countries elements of such legislation may already exist – often in different legal frameworks. Provisions related to cybercrime do not necessarily need to be implemented in one single piece of legislation. With regard to existing structures, it might be necessary to update different pieces of legislation (such as amending an Evidence Act to ensure that it is applicable with regard to the admissibility of electronic evidence in criminal proceedings) or remove provision from an older law (for example in a Telecommunications Act) within the process of introducing new legislation.* Bukan tugas yang mudah untuk memperkenalkan peraturan *cybercrime* karena ada berbagai area yang memerlukan regulasi. Selain hukum pidana dan hukum acara yang substantif, undang-undang *cybercrime* mungkin mencakup masalah yang berkaitan dengan kerja sama internasional, bukti elektronik dan pertanggungjawaban *Penyedia Layanan Internet* (ISP). Di sebagian besar

negara, unsur-unsur perundang-undangan semacam itu mungkin sudah ada-seringkali dalam kerangka hukum yang berbeda. Kejahatan dunia maya *(cybercrime)* ini ketentuannya tidak perlu diimplementasikan dalam satu undang-undang tunggal.(Bunga, 2019, hal. 13) Struktur yang telah ada di dalam undang-undang hanya perlu pembaharuan yang berbeda (seperti mengubah undang-undang bukti untuk memastikan hal itu dapat diterapkan sehubungan dengan diterimanya bukti elektronik dalam proses pidana) atau menghapus ketentuan dari undang-undang yang lebih lawas atau sudah lama (untuk contoh dalam undang-undang telekomunikasi) dalam proses memperkenalkan undang-undang baru.

B. Tinjauan Umum Tentang *Cyber Crime*

1. Pengertian *Cyber Crime*

Perkembangan budaya dapat menjadi alat perubahan di tengah masyarakat, salah satu hasil dari perkembangan budaya yaitu teknologi. Dengan adanya kemajuan teknologi membawa dampak positif dan juga dampak negatif terhadap perkembangan dan peradaban manusia. Dampak positif dalam arti dapat digunakan untuk kepentingan manusia itu sendiri, sedangkan dampak negatif yaitu berkaitan dengan dunia kejahatan.

Ditemukannya komputer sebagai produk ilmu pengetahuan dan teknologi merupakan sebuah perkembangan yang membuat terjadinya *konvergensi* antara teknologi komunikasi, media dan komputer yang menghasilkan sarana dan sistim informasi terbaru yang disebut dengan internet atau jaringan internasional *(International Networking)*, hal ini merupakan

sebuah penemuan terbesar pada abad ke-20. Internet basisnya adalah komputer, dimana *Personal Computer* (PC) dihubungkan dengan menggunakan sebuah sistem jaringan terbaru yang berhubungan langsung dengan satelit komunikasi sehingga terbentuklah jaringan antar *personal computer*. Menurut Abdul Wahid dan Moh. Labib *The US Supreme Court* mendefinisikan internet sebagai *international network of interconnected computers* yaitu sebuah jaringan internasional dari komputer yang saling berhubungan. Dapat dilihat dari definisi tersebut bahwa dimensi internasionalnya yaitu jaringan antar komputer tersebut melewati batas-batas teritorial suatu negara. (Qutub, 2014b, hal. 36)

Berkembangnya zaman membuat adanya kemajuan teknologi informasi dan komunikasi yang modern, manusia mendapatkan kemudahan dam kenyamanan dalam menyebarkan informasi dan menjalin komunikasi dengan orang lain di belahan dunia manapun. Pengaruh internet telah mengubah jarak dan waktu menjadi tidak terbatas. Dengan media internet orang dapat melakukan berbagai aktivitas yang sulit dilakukan dalam dunia nyata *(real)* karena kendala jarak dan waktu. Internet sangat mengubah pandangan manusia terhadap komunikasi dalam bergaul, berbisnis, dan lain sebagainya. Namun kecanggihan teknologi ini juga berpotensi buruk, maksudnya dapat membuat orang cenderung melakukan perbuatan yang bertentangan dengan norma-norma sosial yang berlaku. Kemajuan teknologi informasi dan komunikasi ini telah membawa perubahan yang mendasar terhadap sensitifitas moral masyarakat kita ketika teknologi itu disalahgunakan.(Dewi Karsono, 2011, hal. 13)

Internet merupakan ruang bebas yang mana dalam artian tidak adanya kontrol dari manapun dan tidak ada pusatnya, sehingga hal ini membuat pemerintah suatu negara membatasi penggunaan internet dengan cara melakukan sensor, mendapat tanggapan yang cukup serius dari para *cyberis* diantaranya John Perry Barlow dengan mengeluarkan *Declaration Of Independent of Cyberspace* sebagai bentuk protesnya. Isi deklarasi lebih menekankan pada kebebasan ruang saja yaitu kebebasan di *cyber space* (dunia maya), sedangkan kebebasan para penghuninya tidak dijadikan perhatian pokok.

Dunia maya (*cyber space*) telah menciptakan bentuk kejahatan baru, sebagai dampak negatif yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi dan telekomunikasi yaitu kejahatan yang berkaitan dengan aplikasi internet yang dalam istilah asing disebut *cybercrime* (kejahatan siber) yaitu segala kejahatan yang dalam modus operandinya (cara melakukannya) menggunakan fasilitas internet. Kejahatan ini sering diartikan sebagai suatu kejahatan yang dilakukan dalam ruang atau wilayah siber. (Qutub, 2014b, hal. 3)

Kejahatan siber (*cybercrime*) adalah tidak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat utama dalam melakukan kejahatan. Kejahatan siber merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. *Cybercrime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbassis pada kecanggihan

perkembangan teknologi internet.(Yulianti, 2021, hal. 1) Kejahatan dunia maya atau yang sering disebut dengan istilah *cyber crime* meupakan jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi dan komunikasi tanpa batas, serta memiliki sebuah karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan tingkat keamanan yang tinggi, dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet. (Gani, 2014, hal. 16) *Cybercrime* merupakan kejahatan baru yang sangat berbeda dengan bentuk-bentuk kejahatan konvensional yang selama ini dikenal.

Jenis kejahatan *cybercrime* yang mana menggunakan internet dalam aksinya ini membuat tidak dapat sepenuhnya terjangkau oleh hukum yang berlaku saat ini bahkan tidak dapat sepenuhnya diatur dan dikontrol oleh hukum. *Cybercrime* merupakan suatu istilah umum yang pengertiannya mencakup berbagai tindak pidana yang dapat ditemukan di dalam KUHP atau Perundang-undangan pidana lain yang menggunakan teknologi komputer sebagai suatu komponen sentral. Dengan demikian *cybercrime* dapat berupa: tindakan sengaja merusak *property*, masuk tanpa ijin, pencurian hak milik intelektual, perbuatan cabul, pemalsuan dokumen, pornografi anak, pencurian dan beberapa tindak pidana lainnya. (Qutub, 2014b, hal. 40)

Dari beberapa pengertian yang telah dibahas di atas, *cybercrime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/alat atau komputer sebagai objek,

baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

2. Jenis-jenis *Cyber Crime*

Jenis-jenis *cybercrime* berdasarkan jenis aktivitasnya:

1. *Unauthorized Access to Computer System and Service:* Kejahatan ini dilakukan dengan menyup atau diam diam masuk ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang diksesnya. Biasanya pelaku kejahatan *(hacker)* melakukan hal tersebut dengan mensabotase (melakukan perusakan) ataupun untuk mencuri informasi penting dan rahasia, lalu dapat juga hanya karena ingin melakukan sebuah tantangan untuk mencoba atau mengetes keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin sering terjadi seiring dengan berkembangnya teknologi internet.
2. *Illegal Contents*: Kejahatan ini dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Pemuatan berita bohong atau fitnah merupakan contoh dari kejahatannya. Hal ini dapat membuat hancurnya harkat martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi (membuat gelisah) dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya.

3. *Data Forgery:* Kejahatan ini dilakukan dengan memalsukan data pada dokumen-dokumen penting yang mana tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *ecommerce* dengan seolah-olah membuat terjadinya"salah ketik" yang pada akhirnya akan menguntungkan pelaku.
4. *Cyber Espionage:* Kejahatan ini memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer *(computer network system)* pihak sasaran atau pihak yang dituju. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized* (terkomputerisasi).
5. *Cyber Sabotage and Extortion:* Kejahatan ini dilakukan dengan membuat suatu gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan atau memasukkan suatu *logic bomb* (bom logika), virus komputer ataupun suatu program tertentu. Sehingga dengan hal ini data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Setelah hal tersebut terjadi dalam beberapa kasus, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan

komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber terrorism.*

6. *Offense against Intellectual Property:* Kejahatan ini dilakukan untuk memperoleh hak atas kekayaan intelektual yang dimiliki pihak lain di dalam internet. Sebagai contoh yaitu peniruan tampilan pada *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.
7. *Infringements of Privacy:* Kejahatan ini dilakukan untuk memperoleh informasi dari seseorang yang mana merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized,* yang mana apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, sebagai contoh misalnya nomor kartu kredit, ataupun nomor pin ATM.
8. *Cracking:* Kejahatan ini dilakukam dengan menggunakan teknologi komputer yang mana aksinya dilakukan untuk merusak *system* keamanan suatu *system computer* dan biasanya melakukan pencurian, tindakan anarkis begitu mereka mendapatkan akses untuk masuk. Biasanya manusia sering salah menafsirkan antara seorang *hacker* dan *cracker* dimana *hacker* sendiri identetik dengan perbuatan negatif, padahal *hacker* adalah orang yang senang memprogram dan percaya bahwa

informasi adalah sesuatu hal yang sangat berharga dan ada yang bersifat dapat dipublikasikan dan rahasia.

9. *Carding:* Kejahatan ini dilakukan dengan menggunakan teknologi komputer dalam melakukan transaksi dengan menggunakan *card credit* orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil.(Yulianti, 2021, hal. 2)

C. Tinjauan Umum Tentang *Cyber Terrorism*

1. Pengertian *Cyber Terrorism*

Kata "terorisme" berasal dari bahasa Inggris "*terrorism*". Yang mana diambil dari bahasa Latin "*terrere*" yang berarti "menyebabkan ketakutan". Sehingga kata "teror" itu berarti menakut-nakuti.(Rifaldhi, 2020, hal. 18) Terorisme adalah sebuah ancaman atau tindakan berbahaya yang ditujukan kepada organisasi pemerintahan atau non pemerintahan dengan tujuan politik, keagamaan maupun alasan ideologi. Termasuk dari tindakan ini adalah seperti melakukan tindak kejahatan terhadap orang dan merusak tatanan publik.(Dewi Karsono, 2011, hal. 23) Terorisme telah menjadi kejahatan yang meresahkan bukan hanya pada masyarakat suatu negara, namun juga menjadi keresahan masyarakat internasional. Sifat kejahatan terorisme yang memiliki jaringan internasional dan tingkat mobilitas sangat tinggi serta mengancam keamanan domestik, regional dan internasional menuntut perhatian masyarakat internasional.

T.P. Thornton dalam bukunya *Terror as a Weapon of Political Agitation* yang ditulis pada tahun 1964, menyatakan bahwa terorisme

merupakan: “Penggunaan teror sebagai tindakan simbolis untuk mempengaruhi kebijakan dan tingkah laku politik dengan cara-cara ekstra normal, khususnya penggunaan kekerasan dan ancaman kekerasan. Menurut Thornton, terorisme dapat dibagi menjadi dua macam yaitu, *enforcement terror dan agitational terror*. Bentuk pertama adalah teror oleh penguasa untuk menindas yang melawan kekuasaannya, sedangkan bentuk kedua yaitu, teror yang dilakukan untuk mengganggu tatanan politik yang mapan untuk kemudian dikuasai”. (Dewi Karsono, 2011, hal. 23) Kekerasan atau ancaman kekerasan yang dilakukan pelaku terror diperhitungkan sedemikian rupa untuk menciptakan suasana ketakutan dan bahaya dengan maksud menarik perhatian nasional atau internasional terhadap suatu aksi maupun tuntutan. *RAND Corporation*, sebuah lembaga penelitian dan pengembangan swasta terkemuka di AS, melalui sejumlah penelitian dan pengkajian menyimpulkan bahwa tindakan yang dilakukan para aksi teror merupakan tindakan kriminal. Definisi konsepsi pemahaman lainnya menyatakah bahwa:

(1) Terorisme bukan merupakan bagian dari tindakan perang, sehingga sepatutnya tetap dianggap sebagai tindakan kriminal, juga situasi diberlakukannya hukum perang,
(2) Sasaran utama terorisme adalah sasaran sipil, dengan demikian sasaran militer tidak dapat dikategorikan sebagai tindakan terorisme, dan
(3) Aksi terorisme itu dapat saja mengklaim tuntutan bersifat politis meskipun dimensi politik aksi teroris tidak dapat dinilai,(Natsir, 2009, hal. 74)

Pada 1994 Majelis Umum PBB telah menggambarkan bahwa tindak pidana terorisme merupakan tindak *criminal* yang diperkirakan akan berhasil menciptakan provokasi untuk menciptakan teror pada masyarakat umum. Provokasi ini dilakukan oleh sekelompok orang dengan tujuan politik yang alasannya tidak dapat dibenarkan. Apapun pertimbangan yang dapat digunakan untuk membenarkan mereka yaitu politiknya, filosofis, ideologis, ras, etnis, agama atau sifat lain.(Putri Andini, 2020, hal. 15)

Menurut DCSINT Handbook No.1.02, *Cyber operations and Cyber terrorism,* yang digunakan untuk melatih tantara AS, operasi internet terdiri dari terorisme internet dan dukungan internet, diekspresikan melalui perencanaan, rekrutmen dan propaganda. Dengan aktivitas semacam ini, jaringan *computer* dapat digunakan sebagai senjata, sebagai target perantara atau sebagai aktivitas yang mendahului atau mengikuti serangan fisik. *The Manual* menyatakan bahwa tujuan paling penting dari *cyber terrorism* adalah hilangnya integritas target itu sendiri, mengurangi kemungkinan tindakannya, kurangnya kepercayaan, keamanan, dan keselamatan, dan akhirnya kehancuran fisik. Motivasi paling umum yang diidentifikasikan dalam *cyber terrorism* adalah pemerasan, keinginan untuk dihancurkan, berbagai jenis eksploitasi dan balas dendam. Dan tindakan paling umum yang dilakukan atau diancam oleh teroris adalah penghancuran fisik, penghancuran data dan informasi penting, serangan terhadap system komputer yang sangat penting, serbuan illegal ke dalam sistem komputer dari kepentingan publik dan penolakan akses sistem, layanan, dan data penting.(Putri Andini, 2020, hal. 30)

2. Bentuk-bentuk *Cyber Terrorism*

Para pakar pada *era modern* ini mendefinisikan dan menggambarkan terorisme dalam konteks klasifikasi tipologis sistematis, pembagian jenis terorisme tersebut berbeda berdasarkan motif ataupun media yang digunakan.

Pembagian jenis terorisme berdasarkan motivasi yang ingin dicapai adalah sebagai berikut:

1. Terorisme Baru: Terorisme baru ditandai dengan ancaman serangan skala besar oleh kelompok teroris pembangkang, formasi baru dan kreatif organisasi teroris, solidaritas agama lintas batas, dan pembenaran moral untuk kekerasan politik;
2. Terorisme Negara: Terorisme negara di mana pemerintah melakukan kejahatan terhadap musuh. Terorisme negara dapat diarahkan ke luar melawan musuh di panggung internasional atau ke dalam melawan musuh di dalam negeri;
3. *Counter-Terrorism*: Terorisme yang dilakukan oleh gerakan *non*-negara dan kelompok-kelompok yang menentang pemerintah, kelompok etnis, kelompok agama, dan musuh yang dianggap lainnya;
4. Terorisme Agama: Terorisme agama dimotivasi oleh keyakinan imperatif bahwa kekuatan dunia lain telah mendukung dan memerintahkan penggunaan kekerasan teroris untuk meningkatkan kemuliaan iman. Terorisme agama biasanya dilakukan untuk melindungi apa yang diyakini dan dianggap sebagai satu-satunya keyakinan yang benar;

5. Terorisme Ideologis: Terorisme ini dilatarbelakangi oleh sistem kepercayaan politik (ideologi) yang memperjuangkan hak-hak yang dirasakan sendiri dan melekat pada kelompok atau kepentingan tertentu yang bertentangan dengan kelompok atau kepentingan lain. Sistem kepercayaan menggabungkan pembenaran teoretis dan filosofis untuk secara eksplisit menegaskan hak atau kepentingan kelompok yang diadvokasi; dan
6. Terorisme Internasional: Terorisme telah merambah panggung dunia. Target dipilih karena nilainya sebagai simbol kepentingan nasional atau internasional transnasional dari negara asal. (Putri Andini, 2020, hal. 19)

Unsur-unsur dan bentuk-bentuk *cyber terrorism* antara lain:

1. Serangan bermotif politik yang dilakukan melalui dunia maya, berpotensi menimbulkan korban jiwa;
2. Serangan kekerasan terhadap infrastruktur penting seperti keuangan, energi, transportasi, dan lembaga pemerintah;
3. Serangan yang mempengaruhi fasilitas *non*-esensial, yaitu serangan yang tidak mempengaruhi masyarakat umum, tidak diklasifikasikan sebagai tindakan *cyber terrorism;*
4. Serangan teroris yang berasal dari dunia maya yang menimbulkan ketakutan atau menimbulkan kerugian serius bagi masyarakat luas;
5. Serangan bukan hanya untuk keuntungan pribadi atau uang;
6. Menyebarkan berita bohong tentang kejahatan teroris melalui media sosial; dan

7. Segala bentuk kegiatan teroris, baik yang terorganisir maupun individu, termasuk pembiayaan, propaganda, rekrutmen, pelatihan, perencanaan, melakukan penyerangan, bahkan persembunyian melalui dunia maya.

Secara umum dapat dikatakan bahwa terorisme memerlukan unsur dan bentuk sebagai berikut:

1. Ancaman atau kekerasan;
2. Tujuan atau maksud tertentu;
3. Biasanya membahayakan ketentraman umum;
4. Menimbulkan ketakutan; dan
5. Dampak bagi masyarakat luas.

Tindakan terorisme di Indonesia itu memiliki unsur membuat rasa takut kepada orang lain, dan rasa takut itu juga harus ditujukan kepada orang yang banyak atau *massal*. Seumpama tidak termasuk dari unsur ini, maka kejahatan tersebut hanya masuk di dalam ketentuan pidana biasa. (Dewi Karsono, 2011, hal. 25)

Perencanaan dan pelaksanaan *cyber terrorism* sebenarnya merupakan bentuk komunikasi, dan berlangsung melalui media komunikasi modern (termasuk lokasi), komunikasi jaringan dengan internet sebagai tulang punggungnya. Oleh karena itu, penulis mengelompokkan situasi ini hanya dalam bentuk komunikasi:

1. Propaganda: Menurut Thackrah (2004), “Propaganda adalah informasi, gagasan, doktrin, atau ajakan khusus yang disebarkan untuk

mempengaruhi pendapat, perasaan, sikap, atau perilaku kelompok tertentu, baik secara langsung maupun secara metodis dapat didefinisikan: digunakan secara tidak langsung untuk mendapatkan keuntungan dari sponsor." (dalam *slide* kuliah dinamika terorisme) Oleh karena itu, propaganda dapat digunakan untuk mempengaruhi pendapat, tindakan, atau tindakan suatu kelompok tertentu. Penularan propaganda dapat secara langsung maupun tidak langsung. Propaganda dilakukan dengan tujuan untuk menyampaikan pesan itu sendiri, seperti aktor teroris lainnya, rekrutan, atau kader dan simpatisan. Propaganda teroris dapat ditemukan di berbagai media, termasuk internet. Internet menjadi media peluang bagi pelaku dan kelompok teroris untuk melakukan kegiatan propaganda. Beberapa kemungkinan tersebut adalah:

(1). Internet menawarkan kesempatan kepada publik untuk merangkul ideologi radikal. Jangkauan yang lebih luas menguntungkan bagi pelaku, kelompok, atau organisasi teroris, dan

(2). Internet membantu meradikalisasi massa. Penonton dihadapkan pada ide-ide radikal tanpa harus berhadapan langsung dengan teroris besar dan radikal mereka. Propaganda terorisme yang paling sering dilakukan adalah penggunaan metode propaganda akta (propaganda yang dilakukan melalui tindakan kekerasan), dehumanisasi, bahkan metode tidak beriman. Menurut *United Nations on Drugs and Crime* (2012), bentuk-bentuk propaganda terorisme antara lain (*slide* kuliah dinamika terorisme).

2. Persentasi Perspektif: Menyajikan sudut pandang bentuk propaganda ini dimaksudkan untuk menyampaikan pandangan atau idealisme pelaku teroris kepada publik. Perspektif ini disampaikan kepada penonton sebagai pesan atau kesaksian yang disebarluaskan untuk meningkatkan kekuatan mereka dengan menimbulkan ketakutan dan kepanikan, pesan itu diposting di YouTube setelah bom Poso.
3. Indoktrinasi: dilakukan untuk mencapai keberhasilan suatu kelompok atau organisasi teroris dengan cara memprovokasi masyarakat untuk ikut serta atau paling tidak mendukung aksi teroris yang dilakukan oleh kelompok atau organisasi teroris tersebut. Indoktrinasi hadir dengan menghadirkan perspektif yang dilakukan oleh teroris sebelum atau sesudah melakukan serangan teroris di dunia nyata.
4. Radikalisasi: dipahami sebagai proses indoktrinasi. Ketika seseorang dihadapkan pada paham dan paham radikal, mereka lebih cenderung percaya, percaya, dan bertindak sesuai dengan keinginan radikal. Hal ini dapat berupa tindakan kekerasan, partisipasi dalam pengeboman, dan lain sebagainya.
5. Propaganda Rekrutmen: hasil yang dicari teroris setelah radikalisasi dan indoktrinasi. Saat ini, adopsi internet sedang meningkat. Contoh propaganda terkait rekrutmen adalah rekrutmen calon syahid atau pelaku bom bunuh diri oleh kelompok bersenjata Iran melalui *website Insight Online Magazine.* Tujuannya adalah untuk melakukan bom bunuh diri terhadap warga AS dan Israel.

6. Rekrutmen: dilakukan untuk menyebarkan ideologi dan mencari dukungan dan simpati publik. Konsentrasi pengunjung *website* dan informasi *online* menjadi sasaran teroris melalui interaksi dengan calon anggota melalui *chat*, email, dll. Rekrutmen adalah agenda teroris untuk mengumpulkan dukungan untuk populasi atau komunitas yang ditargetkan. Rekrutmen, seperti semua bentuk propaganda, ditujukan untuk menarik simpatisan untuk bergabung dengan jaringan dan organisasi teroris. Juga menggunakan materi yang beredar di Internet untuk melatih dan mempersiapkan para pemimpin teroris. Metode rekrutmen dilakukan oleh teroris melalui internet. Media sosial seperti facebook digunakan untuk merekrut bakat. Salah satu kasus terpanas terjadi pada tahun 2014 ketika saksi yang sebelumnya direkrut dan dikirim ke Suriah diinterogasi. Saksi mengaku pernah berteman melalui *wall* facebook dan *chat* facebook dan diberi kesempatan untuk pergi ke suriah.
7. Penyediaan Logistik: saat memberikan logistik ke jaringan teroris, dunia maya biasanya digunakan sebagai sarana untuk mengakses bahan-bahan logistik seperti bahan peledak, senjata, dan bom yang akan dilepaskan. Jaringan teroris biasanya menggunakan dunia maya sebagai alat untuk mengatur akomodasi keberangkatan, terutama jika jaringan teroris berhasil merekrut calon eksekutif melalui media sosial.
8. Pelatihan: kelompok teroris menggunakan dunia maya sebagai kendaraan untuk mencapai tujuan pelatihan mereka. Model pelatihan teroris secara garis besar dapat dibagi menjadi dua kategori: unggahan konten melalui *e-*

book, dan tutorial melalui video dan blog. Saat ini model komunikasi antara calon atau mentor kelompok teroris berjalan melalui forum dan *instant messenger.* (slide kuliah tentang dinamika terorisme) Teroris menggunakan *instant messenger* dan forum untuk mempromosikan materi pelatihan yang tersedia untuk masyarakat umum dan pengguna Internet. Forum internet biasanya disalahgunakan untuk menampilkan tautan ke situs *web* dengan materi penelitian. Selain forum dan instant messenger, teroris juga menggunakan blog dan *e-book* yang dapat diunduh melalui *file sharing* seperti *Shared* dan *Hotfiles.* Teroris kemudian dapat mengunggah video melalui situs penyiaran video seperti YouTube yang menjelaskan cara membuat detonator atau perakitan bom untuk aksi teroris. Selain itu, teroris telah membuat blog untuk memberikan materi tentang Ayah. Ayah adalah persiapan sebelum melakukan aksi terorisme. Berdasarkan studi anekdot tahun 2000, kemampuan teroris atau kelompok untuk membuat bom dikatakan telah diwarisi dari mereka yang menyaksikan perang di Afghanistan. Pelajari cara membuat bom sendiri. Posisi ini cenderung mengakibatkan para pelaku teroris dapat minggir dan bertindak atas inisiatifnya sendiri meskipun tidak ada perintah untuk membimbing atau mengarahkannya. Hal ini dimaksudkan untuk membantu dalam proses mengungkap dan menyabotase banyak jaringan komputer yang diyakini menghalangi mobilisasi mereka untuk menyebarkan propaganda teroris. Internet digunakan untuk menyebarkan materi pelatihan, teknik peretasan,

dan menggunakan perangkat lunak dan metode komunikasi yang sensitif *(enkripsi, anonimitas, deaddrops).*

9. Pembentukan Paramiliter Melawan Secara Hukum: untuk Teroris membutuhkan profil tinggi untuk memobilisasi masyarakat untuk mendukung aksi teroris. Hal ini berkaitan dengan ajakan atau seruan untuk mengerahkan, menggunakan senjata dan membentuk kelompok tempur melalui internet dan media sosial.
10. Perencanaan: menentukan strategi, taktik, dan operasi untuk merencanakan dan mengeksekusi kelompok teroris dengan menggunakan teknologi informasi. Sebuah rencana yang dilakukan oleh aktor, kelompok, atau organisasi teroris dimulai dengan komunikasi rahasia dan akses informasi yang bebas. Komunikasi sensitif mencakup email, pesan terenkripsi, dan ruang obrolan. Informasi seperti peta satelit, informasi pemerintah, rencana transportasi, dan laporan keamanan (tren terorisme) kini tersedia secara gratis. Penggunaan aplikasi Internet pada dasarnya merupakan ancaman terkait penggunaan informasi oleh kelompok teroris untuk tujuan penyebaran terorisme. Salah satu contohnya adalah penggunaan sumber terbuka seperti Google *Earth* dan Google *Maps* oleh milisi Irak ketika merencanakan serangan. Aplikasi akses gratis ini relatif murah karena dapat diakses secara gratis. Di sisi lain, perencanaan juga dapat dilakukan dari percakapan email. Rencana email dapat lebih rinci karena bersifat pribadi, dan Anda dapat dengan bebas menggambarkan pengaturan untuk

melakukan tindakan teroris. Kedua, kelompok teroris sekarang menggunakan program enkripsi untuk melindungi file sensitif.

11. Pelaksanaan Serangan: eksekusi serangan atau eksekusi yang dilakukan oleh kelompok teroris melalui internet sebagai perantara atau media. Secara umum, eksekusi mengikuti pola ini:
    (1). Ancaman kekerasan itu nyata dan pelaksanaannya melibatkan penggunaan senjata,
    (2). Menyebar di internet menimbulkan ketakutan, kecemasan dan kepanikan di masyarakat, dan
    (3). Panggilan video digunakan sebagai pengawas atau pengontrol *real-time* atau *live-action.*

    Berdasarkan pola tersebut, kita dapat memahami bahwa bentuk penggunaan internet seperti ini biasa terjadi di kalangan kelompok teroris. Tindakan kekerasan biasanya dilakukan oleh kelompok teroris dan ditampilkan melalui situs *web* dan siaran video. Penggunaan senjata api juga diperlihatkan seolah-olah dapat menimbulkan ketakutan dan kekhawatiran pada penonton yang menontonnya. Tujuan penyebaran terorisme adalah untuk menarik perhatian publik atas keberadaan mereka. Selain itu, ia memperingatkan publik bahwa aksi terorisme yang sebenarnya akan terjadi. Tindakan teroris dilakukan terhadap target yang telah ditentukan, namun serangan ini juga dipantau dan dikendalikan melalui panggilan video. Rencana serangan didistribusikan secara luas melalui situs web seperti

anshar.net. Halaman ini menjelaskan dan menjelaskan serangkaian aksi teroris yang direncanakan dalam peta lokasi dan target.

12. Persembunyian: setelah pelaksanaan atau eksekusi suatu tindakan terorisme, dilakukan tahapan penyembunyian. Fase ini berusaha menyembunyikan identitas individu atau kelompok teroris dari otoritas publik dan penegak hukum. Hal ini menciptakan kekosongan hukum untuk mengelola kejahatan *cyber terrorism,* menurut analisis hukum yang berlaku di Indonesia.

Indonesia sudah memiliki undang-undang ITE untuk mengatur kejahatan di bidang komputer, tetapi undang-undang tersebut dianggap tidak memadai untuk memerangi terorisme dunia maya. Hal ini dikarenakan UU ITE hanya mengatur satu bentuk *cyber terrorism,* namun UU ITE tidak secara substansial mengatur ketentuan penuntutan tindak pidana *cyber terrorism.* Terorisme yang menggunakan kemajuan informasi sebagai wahana untuk melakukan kegiatan 9P seperti propaganda, rekrutmen, provisi logistik, pelatihan, pembentukan personel militer ilegal, perencanaan, melakukan serangan teroris, penyembunyian dan pendanaan. (Bambang A.S. & Fitriana, 2017, hal. 6)