PAULUS Law Journal
Volume 1 Nomor 2, Maret 2020
e-ISSN : 2722-8525

PENANGGULANGAN CYBER-TERRORISM MELALUI WEBSITE RADIKAL DALAM PERSPEKTIF DEMOKRASI PANCASILA

Gracesy Prisela Christy
Universitas Kristen Indonesia Paulus; Gpchristy@ukipaulus.ac.id

Abstrak
Cyber-Terrorism masuk dalam kategori kejahatan lintas batas negara yang terorganisir dan telah ditetapkan sebagai kejahatan luar biasa.Analisa menunjukan bahwa *Cyber-terrorism* merupakan bentuk transformasi terror yang dilakukan oleh teroris dengan menjadikan jaringan internet sebagai alat atau sasaran serangan. Jenis kejahatan ini bermetamorfosis menjadi kejahatan yang bersifat lintas negara. Pelakunya bisa berasal dari wilayah negara mana saja yang berakibat hukum pada identitas yang berimplikasi pada penentuan jurisdiksi pengadilan. Akibat makna-makna negatif yang dikandung oleh perkataan "*teroris*" dan "*terorisme*" para teroris umumnya menyebut diri mereka sebagai separatis, pejuang pembebasan, militan, mujahidin, dan lain-lain. Dengan rangkian jalur yang cukup maju ini maka dibutuhkan kerjasama yang bersifat global atau internegara. Salah satu solusinya setiap negara harus melakukan sinkronisasi tentang peraturan perundang-undangan yang khusus mengatur tentang *Cyberterror*.
Kata Kunci : Cyber-terrorism; Website Radikal, Demokrasi Pancasila

Abstract
Cyber-Terrorism is included in the category of organized transnational crime and has been determined as an extraordinary crime. The analysis shows that Cyber-terrorism is a form of terror transformation committed by terrorists by making the internet as a tool or target of attacks. This type of crime metamorphoses into a transnational crime. The culprit may come from any region of the country that has legal consequences on identity that have implications for the determination of the court's jurisdiction. As a result of the negative meanings contained by the words "terrorist" and "terrorism" terrorists generally refer to themselves as separatists, liberation fighters, militants, mujahideen, and others. With this fairly advanced pathway sequence, global or international cooperation is needed. One solution is that each country must synchronize the laws and regulations specifically governing Cyberterror.
Keywords : Cyber-terrorism; Radical Websites, Pancasila Democracy

1. Pendahuluan

Dunia pada hari ini, telah menjadi lebih terhubung oleh teknologi informasi dan komunikasi daripada sebelumnya. Sistem telekomunikasi dan komputer dapat terhubung secara global (have global reach)[1] baik mentransfer suara dan data digital yang melintasi batas-batas negara. Sistem tersebut juga menjadi penggerak untuk

[1] Andrew Michael Colarik, *Cyber Terrorism:Political and Economic Implications*, Idea Group Publishing, USA, hal. 11

mendukung pengembangan infrastruktur ekonomi dan industri transportasi, termasuk perdagangan dan layanan pemerintah.

Manfaat kemajuan teknologi informasi dan komunikasi khususnya internet telah menyentuh semua sisi kehidupan manusia modern. Sisi positif ini ternyata diikuti sisi gelap (dark side)[2] penggunaan internet. Internet telah mengalami evolusi, yang semula digunakan untuk kepentingan militer dan ilmiah menjadi sasaran dan sarana kejahatan. Para pengguna internet tidak saja hanya para ilmuwan, pengguna umum melainkan dipakai oleh mata-mata dan teroris.

Melihat ketergantungan yang cukup besar terhadap internet maka serangan teroris yang ditujukan kepadanya menjadi ancaman serius yang termasuk wilayah baru bagi keamanan nasional dan kebijakan publik. Oleh karena itu, ketika suatu Negara ketika ingin beranjak pada e-link segala urusan yang bersifat publik sebagai kepentingan nasionalnya maka negara tersebut harus mulai memikirkan untuk mengamankan sistem jaringannya dari serangan, khususnya dari cyberterrorism. Maka sangat penting fenomena cyberterrorism dipahami dengan baik karena bayang-bayang serangan terorisme yang selalu mengintai kita semua setiap saat.

Sisi lain yang perlu dicermati yaitu adanya kecenderungan dari para ahli yang menganggap cyberterrorism sebagai kejahatan dunia siber biasa. Anggapan seperti ini tidak saja menjebak kita untuk bersikap menyederhanakan persoalan melainkan juga berakibat pada kualitas respon antisipatifnya menjadi lamban dan terkesan tidak serius. Padahal jika ditilik secara mendalam penggunaan jaringan internet berkorelasi positif dengan transformasi jaringan teror yang awal keanggotaannya terbatas pada wilayah tertentu berubah menjadi massal dan berskala global.

Untuk itu, diperlukan pemahaman yang memadai mengenai anatomi cyberterrorism . Keutuhan pemahaman mengenai kejahatan yang tergolong baru ini menjadi penting untuk membuat peta jalan yang komperehensif untuk meminimalisir kemampuan teroris untuk melakukan serangan terhadap jaringan ataupun menjadikan komputer sebagai media untuk propaganda teror. Informasi yang didapat secara cepat, tepat dan akurat memainkan peranan sangat penting dalam berbagai aspek kehidupan manusia, seperti penentuan sebuah kebijaksanaan, sebagai alat bantu dalam proses pengambilan keputusan atau bahkan sebagai tren atau gaya hidup manusia modern. Kenyataannya semakin banyak kalangan bisnis, organisasi, perkantoran, pendidikan dan militer hingga individu yang menjadi sangat ketergantungan dengan fenomena zaman informasi ini. Sehingga munculah istilah yang sering dikenal dengan sebutan "the information age" atau abad informasi.

Namun kenikmatan serta kemudahan yang ditawarkan abad informasi sekaligus mengundang para terorisme di dunia maya (cyber terrorism) untuk turut serta

[2] Lukasz Jachowicz, *Cyberterrorism And Cyberhooliganism: How To Prevent And Fight International and Domestic*, paper presented at Collegium Civitas Foreign Policy of the United States of America, January 2003, hal. 1.

berpetualang didalamnya. Pengertian tentang cyber terrorism sebenarnya terdiri dari dua aspek yaitu cyber space dan terrorism, sementara para pelakunya disebut dengan cyber terrorists. Para hackers dan crackers juga dapat disebut dengan cyber terrorist, karena seringkali kegiatan yang mereka lakukan di dunia maya dapat menteror serta menimbulkan kerugian yang besar terhadap korban yang menjadi targetnya, mirip seperti layaknya aksi terorisme. Keduanya mengeksploitasi dunia maya untuk kepentingannya masing-masing. Ada perbedaan tipis antara cyber terrorist dan hackers hanyalah pada motivasi dan tujuannya saja, dimana motivasi dari para cyber terrorist adalah untuk kepentingan politik kelompok tertentu dengan tujuan memperlihatkan eksistensinya di panggung politik dunia. Sementara motivasi para hackers atau crackers adalah untuk memperlihatkan eksistensinya atau adu kepintaran untuk menunjukan superiotasnya di dunia maya dengan tujuan kepuasan tersendiri atau demi uang.

Di negara demokrasi, dimana negara melayani rakyat dengan mengakui kebebebasan pendapat dan menyerap aspirasi dari rakyatnya, ini akan menjadi pisau bermata dua. Satu sisi, rakyat akan merasa puas dengan negaranya dan akan loyal pada negaranya. Rakyat akan bahu-membahu berkontribusi membantu pemerintah membangun dan menjaga kekondusivan negara. Namun di lain sisi, ada kemungkinan negara akan kewalahan dalam menuruti apa yang diminta rakyatnya dan bahkan tidak bisa memenuhi permintaan. Akhirnya, rakyat akan semakin marah dan tiba pada akhirnya gerakan separatis akan semakin meluas dan kekuatan (power) negara akan melemah. Jika ini terjadi, sikap antipasti terhadap pemerintah akan memicu tindakan-tindakan menentang pemerintah berupa terror-teror kepada negara.[3]

2. Metode

Penulisan artikel ini menggunakan metode penelitian hukum dengan pendekatan yuridis normatif dengan mengacu pada norma-norma hukum positif dan nilai nilai pancasila. Data yang digunakan dalam artikel ini adalah data sekunder berupa bahan hukum primer yaitu norma hukum positif , dan bahan hukum primer yaitu literatur berupa buku, jurnal, dan artikel terkait. Analisis data dalam artikel ini menggunakan analisis kualitatif dengan mendeskripsikan fakta-fakta yang ada, kemudian dilakukan analisis berdasarkan norma hukum positif maupun teori yang ada.

3. Penggunaan Teknologi Informasi dan Perubahan Perilaku Budaya Hukum

Masyarakat Indonesia memasuki pergaulan Internasional melalui media internet dengan berbagai pola komunikasi dalam kemajuan teknologi. Kemajuan teknologi informasiitu ditandai dengan kehadiran perangkat keras bernama komputer dan

[3] *faizbmarwan/560d3e78349773ef0b6b5009/keterkaitan Antara demokrasi-dan-terorisme//page=all*

perangkat lunak program internet. Definisi komputer dari Institut Komputer Indonesia adalah suatu rangkaian peralatan dan fasilitas yang bekerja secara elektronik, dibawah kontrol suatu system pengoperasian (operating system) untuk melaksanakan pekerjaan berdasarkan rangkaian instruksi yang disebut program, serta mempunyai media penyimpanan di dalam mesin (internal storage) yang digunakan untuk menyimpan operating system, program dan data yang diperoleh. Sementara itu internet merupakan program atau perangkat lunak (software) yang membentuk sistem pengoperasian (oeprating system) dan peralatan itu digunakan sebagai alat proses data elektronik, magnetik, optikal, untuk melaksanakan fungsi logika, aritmetika, penyimpanan, dan penemuan data kembali.

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 masayarakat 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. Perilaku hukum bukan hanya berarti taat hukum, tetapi semua perilaku yang merupakan reaksi terhadap sesuatu yang sedang terjadi dalam sistem hukum (*reacting to something going on the legal system)* sehingga tidak mentaati hukum yang diberlakukan dalam sistem kehidupan masyarakat sosial[4].

Kaitannya perilaku hukum dalam kehidupan masyarakat bukan hanya reaksi taat,*(obey)* dan tidak taat *(disobery)* melainkan juga reaksi menggunakian (*use)* atau tidak menggunakan *(not use)* terhadap suatu aturan hukum.Kemanfaatan media (*the covergance media)* membawa perubahan pada perilaku dalam penggunaan teknologi informasi, ketika setiap orang tidak mampu memahami hakikatperubahan dalam

[4] Josua Sitompul, (2012), *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*. Tatanusa, Jakarta.

bidang teknologi informasi itu[5]. 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.

Terminologi cybercrime menunjukan bahwa kejahatan yang dilakukan itu ada dalam ranah cyberspace. Kejahatan yang berbasis pada teknologi informasi dengan menggunakan media komputer sebagaimana terjadi saat ini, dapat disebut dengan beberapa istilah yaitu computer misuse, computer abuse, computer fraud, computer – related crime, computerassisted crime, atau computer crime . Kejahatan yang menggunakan teknologi informasi dengan alat yang dikenal sebutannya komputer itu menurut penulis adalah segala bentuk kejahatan yang dilakukan dengan pola komputerisasi melalui jaringan dan para penggunanya.

Kejahatan dunia maya atau cybercrime dengan menggunakan teknologi informasi kecanggihan komputer itu, dari pandangan keilmuan secara umum dibagi dalam 2 (dua) kategori yaitu :

A. Cybercrime dalam pengertian sempit adalah kejahatan terhadap penggunaan system komputer;
B. Cybercrime dalam pengertian luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer[6].

Perubahan di dalam masyarakat telah terjadi, batasan wilayah hukum masyarakat satu negara dengan negara lain telah terlampaui oleh kegiatan di ruang dunia maya yang membawa berbagai dampak hukum akibat perilaku budaya hukum yang juga telah berubah. Di dalam hal ini perlu disikapi dengan tegas oleh pemerintah atas dampak dari perubahan perilaku budaya hukum yang ada dengan membatasi penggunaan teknologi dalam hal pengawasan secara ketat terhadap provider yang ada dan beroperasi di Indonesia. Kondisi ini sudah banyak dilakukan oleh negara tetangga seperti malaysia, singapura dan Negara tetangga lainnya yang lebih tegas dalam hal mengawal dan megawasi beroperasinya para owner dari provide yang ada. Situasi tesebut dilakukan guna mengurangi tingkat kejahatan yang terjadi di ruang dunia maya akibat dari perilaku pengguna dengan perilaku yang tidak pada kepantasan dan menyimpang dalam menggunakan sarana perangkat lunak dan keras komputer.

Ketegasan sikap itu diperlukan ketentuan peraturan perundang-undangan hukum media yang memiliki subtansi tegas dalam melindungi kepentingan kemanan Negara Kesatuan Republik Indonesia, sekaligus melindungi warga negara dalam

[5] Golose, Petrus Reinhard. (2015), *Invasi Terrorisme Ke Cyberspace*, YPKIK, Jakarta

[6] Romli Atmasasmita, (2003), *Aspek Nasional Dan Global Pemberantasan Terorisme*, Jurnal Hukum Internasional., v2n3

kemanan diri sebagai pengguna dari ruang cyber, meski Indonesia telah memiliki satu Undang-Undang berkaitan dengan Telekomunikasi yaitu Undang-Undang Informasi dan Transaksi Elektronik yang telah mengakomodir mengatasi kejahatan cyber atau cyber crime.

4. Penegakan Hukum atas Tindak Pidana Cyber Terrorism dalam Hukum Nasional

Aksi teorisme 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. 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 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 dimasukan 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 (convergance 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 pemangunan hukum nasional mengapresiasi hadirnya cyber law secara terintgrasi akan menjadi

sebuah penguatan kepastian hukum yang lebih baik, mengingat banyak sekali gerakan terkait tindak pidana terorisme semakin berkemang dengan berbagai pola komunikasi dalam kemanfaatan media yang ada, sebagai alat komunikasi untuk melakukan aksi kejahatannya. Di dalam ketentuan Undang-Undang Nomor 15 Tahun 2003 tentang Terorisme dapat digunakan untuk menjerat pelaku Cyber Terrorism karena terdapat Pasal yang mengatur tindak pidana terrorism 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 walaupan tindak pidana terorisme belum terjadi atau baru hanya sampai pada tahap dengan maksud atau dengan tujuan atau merencanakan tindak pidana terorisme. Untuk 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 batuan 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. 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[7] :

a. *Ketentuan "roving wiretap" agar departemen kehakiman memiliki kekuasaan untuk menyadap guna menelusuri jejak para tersangka tanpa mengindahkan telepon yang mereka gunakan.*
b. *Memperkenalkan sharing informasi yang semula dilindungi oleh grand jury di antara aparat intelejen dan aparat penegak hukum Memperkenankan penyitaan pesan-pesan voicemail sesuai dengan surat perintah (warrant)*

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[8].

Saat ini telah dilakukan upaya oleh kementerian POLHUKAM, Hukum dan HAM, dan lembaga terkait lainnya seperti Badan Nasional Penanggulangan Teroris (NCTA National Counter Terrorism Act) untuk melakukan revisi terhadap Undang-Undang Nomor 15 Tahun 2003 yang dalam kebutuhan terhadap penanganan tindak pidana terorisme telah berkembang dengan penggunaan alat teknologi bernama komputer, dan perilaku kejahatannya telah berubah pola dengan penyalahgunaan alat teknologi komunikasi dan informasi tersebut, hingga lahir istilah cyber crime dalam tindak pidana cyber terrorism.[9]

Termasuk juga Basrief Arief[10] yang menyatakan "Terorisme merupakan kejahatan luar biasa (extra ordinary crime) yang membutuhkan pola penanganan yang luar biasa pula (extra ordinary measure) yang berbeda dengan penanganan tindak pidana pada umumnya". Maka kondisi itu melahirkan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1Tahun 2002 yang kemudian menjadi Undang-Undang Nomor 15 Tahun 2003.

5. Pencegahan terhadap Cyberterrorism: Menekan Penyebaran dan Pertumbuhan Propaganda

Demokrasi berasal dari bahasa Yunani yang diambil dari kata "demos" (rakyat) dan "kratos" (pemerintahan). Sebagai bentuk pemerintahan, demokrasi bertolak belakang dengan monarki (diperintah oleh raja, ratu, atau kaisar), oligarki (diperintah

[7] Abdul Hakim G. Nusantara, (2003), *Undang-Undang Pemberantasan Tindak Pidana Terorisme Dalam Perspektif Negara Hukum*, Badan Pembinaan Hukum Nasional, Bandung, hal.1.
[8] Romli Atmasasmita, *Op.cit*, 11
[9] Abdul Hakim G. Nusantara, Op.cit
[10] Kejaksaan Agung Republik Indonesia, (2013), *Panduan Penanganan Perkara Tindak Pidana Terorisme* Kejaksaan Agung Republik Indonesia, Jakarta, hal. 5

oleh beberapa orang), aristokrasi (diperintah oleh kelas istimewa), dan despotisme (pemerintahan absolut oleh satu orang)[11].

Komunikasi yang terjadi adalah komunikasi satu arah. Komunikasi satu arah berarti tidak ada interaksi langsung antara komunikator dan komunikan (Matusitz, 2012). Setiap informasi yang ditransfer oleh komunikator (media massa) akan menempatkan komunikan (pembaca) dalam posisi pasif. Dalam situasi seperti itu, pembaca tidak akan bisa menolak kenyataan yang dikonstruksi oleh media massa, padahal sebenarnya "kenyataan" bukanlah yang sebenarnya terjadi.

Dalam konteks propaganda radikalisme dan terorisme, media massa membangun sebuah realitas yang berbeda dengan realitas sosial kehidupan sehari-hari. "*tujuan propaganda teroris yang menyebar di media massa adalah 1) mempromosikan kekerasan, 2) mempromosikan retorika para ekstremis yang mendukung kekerasan, 3) rekrutmen, 4) hasutan dan 5) radikalisasi*".

Propaganda terorisme menganjurkan bahwa kekerasan dapat dibenarkan. Kekerasan ini termasuk tindakan terhadap pemerintah, membunuh warga sipil dan bahkan perempuan dan anak-anak. Dalam beberapa pandangan radikal yang diadopsi oleh kelompok-kelompok teroris seperti Jama'ah Islamiyah, terorisme telah menjadi sesuatu yang harus dilakukan untuk setiap individu. Mereka percaya bahwa membunuh orang lain jika diperlukan, dibenarkan dalam "jihad"[12].

Propaganda terorisme juga bertujuan untuk menghasut pengguna internet dengan informasi dan pemahaman yang menyesatkan. Informasi dan pemahaman ini dalam bentuk penyalahgunaan istilah agama untuk membenarkan teroris dengan tujuan merekrut anggota baru. Pengguna internet cenderung menggunakan jaringan sosial, browsing dan pesan instan, menyebabkan 80% pengguna internet sangat rentan dan berpotensi dipengaruhi oleh kelompok-kelompok teroris radikal (BNPT, 2016).[13] Tujuan akhir dari propaganda terorisme adalah untuk meradikalisasi orang. Radikalisasi yang terjadi melalui media internet dapat terjadi secara mandiri (self-radicalisation atau radikalisasi diri), ini berarti seseorang dapat menjadi radikal di mana pun mereka berada, bahkan tanpa harus berhadapan langsung dengan kelompok radikal seperti mengikuti dakwah. Seseorang dapat menjadi radikal bahkan ketika dia mengakses informasi yang terdistorsi melalui media internet. Masalah pemberantasan terorisme dikategorikan ke dalam tiga aspek: pencegahan, penegakan hukum dan deradikalisasi. Dalam masalah pencegahan, hal penting yang perlu diatur dalam undang-undang adalah mengkriminalkan semua bentuk tindakan yang mengarah pada tindakan terorisme. Menurut Moghaddam (2005), ada 'tangga' atau tahapan yang menyebabkan seseorang menjadi teroris. Tahapan-tahapan ini

---

[11] "*Demokrasi Pancasila: Pengertian dan Keunggulannya", https://www.kompas.com/skola/read/2020/04/03/121500469/demokrasi-pancasila--pengertian-dan keunggulannya?page=all*.

[12] Golose, Petrus Reinhard. (2015), *Invasi Terrorisme Ke Cyberspace*, YPKIK, Jakarta.

[13] Andi Hamzah. (1989), *Aspek-Aspek Pidana Di Bidang Komputer*. Ghalia, Jakarta

dimulai dengan "interpretasi psikologis" ketika seseorang mulai terkena terorisme dan ideologi teroris; maka intensitasnya lebih tinggi hingga puncaknya adalah untuk melakukan aksi nyata teroris[14].

Di Indonesia, contoh nyata dari tahap ini adalah apa yang disebut "i'dad" atau "persiapan" atau "pelatihan". Kelompok-kelompok teroris itu mendoktrin anggota bahwa "tidak ada jihad tanpa i'dad" atau "tidak ada tindakan tanpa persiapan". Persiapan yang dimaksud, dalam hal ini, adalah pelatihan militer. Kelompok ini diketahui telah mengadakan pelatihan militer di Aceh menggunakan senjata api buatan sendiri di Aceh pada tahun 2010. Di bawah UU Darurat No. 12 Tahun 1951 kelompok itu ditangkap dan senjata-senjata mereka disita sebagai barang bukti.

Belajar dari pengalaman itu, pelatihan saat ini dengan tujuan yang sama dilakukan di hutan dan gunung yang disamarkan sebagai berkemah. Mereka juga menggunakan senjata udara atau bahkan senjata kayu yang disamarkan sebagai permainan. Tidak ada undang-undang yang menetapkan bahwa seseorang bersalah berkemah atau bermain dengan senapan airsoft, ini menjadi sangat berbahaya karena tujuan kelompok ini adalah untuk melakukan i'dad untuk melakukan operasi "amaliyah" yang dapat dilakukan dengan tepat. ditampung meski latihan dilakukan dengan menggunakan senjata baru.

Sampel lainnya adalah jumlah orang yang pergi ke negara-negara seperti Irak dan Suriah. Mereka berangkat dengan alasan ziarah atau liburan, tetapi di sana mereka bergabung dengan ISIS dan komunitas simpatisan lainnya. Tidak ada undang-undang yang menetapkan bahwa seseorang bersalah atas ziarah atau berlibur ke mana pun dia inginkan, sehingga hal ini menjadi sangat berbahaya karena mereka akan semakin terekspos kepada radikalisme. Ketika mereka kembali ke Indonesia, mereka siap untuk merancang dan melakukan aksi teror.

Skeptisisme tentang pentingnya mengatur dan memperluas otoritas lembaga penegak hukum dalam mencegah aksi teror berasal dari pertimbangan bahwa dalam peraturan tersebut adalah multi-tafsir, misalnya terkait definisi tindakan yang dapat dikategorikan ke dalam tindakan terorisme. Pasal dengan banyak celah interpretasi tersebut berpotensi menimbulkan subjektivitas di antara para petugas penegak hukum, sehingga dapat disalahgunakan oleh oknum yang tidak bertanggung jawab untuk mengkriminalkan seseorang atau kelompok tertentu. Hal ini juga berlaku pada kasus pemblokiran situs-situs yang dianggap "radikal" oleh pemerintah, di mana sebagian masyarakat merasa bahwa pembatasan hak atas informasi tidak sesuai dengan nilai-nilai demokrasi yang dianut oleh bangsa Indonesia.

Pada dasarnya, konstruksi setiap peraturan selalu mempertimbangkan dua aspek: keamanan nasional dan kebebasan sipil. Dua hal ini selalu ada dalam zero-sum game; jika kita memperkuat keamanan nasional, secara otomatis akan melemahkan

[14] Bhakti, A. S. (2016). *Deradikalisasi Dunia Maya, Mencegah Simbiosis Terorisme dan Media*, Daulat Press, Jakarta

kebebasan sipil, dan sebaliknya (Wark, 2006: 2). Kedua hal ini selalu berada pada satu continuum line (garis kontinum) yang dapat bergeser sesuai kebutuhan. Karena itu, pemerintah harus menemukan keseimbangan dari kedua hal ini agar kehidupan negara dapat berjalan dengan baik.

Jika pemerintah merasa ada ancaman terhadap keamanan nasional, maka jangan ragu untuk mengorbankan kebebasan sipil termasuk memblokir situs-situs radikal. Tetapi jika situasinya dirasakan cukup aman, kebebasan sipil dapat ditingkatkan dan secara otomatis mengorbankan keamanan nasional; akibatnya, akan muncul kerawanan serangan teror. Penghargaan atas hak asasi manusia harus diprioritaskan, tetapi jangan sampai ini membuat kita lupa bahwa terorisme adalah kejahatan luar biasa yang membutuhkan pendekatan luar biasa juga. Pendekatan luar biasa harus relevan dengan semangat demokrasi dan hak asasi manusia sehingga efektif, efisien dan tetap humanis.

Dari hasil riset dan survey serta berbagai laporan tentang kejahatan komputer yang terjadi sekarang ini, diketahui bahwa saat ini tidak ada satupun jaringan komputer yang dapat diasumsikan 100% persen aman dari serangan virus komputer, spam, email bom dan sebagainya dari para hackers dan cyber terrorist. Seorang hacker atau cyber terrorist yang sudah berpengalaman dapat dengan mudah melakukan 'breaks-in' atau memasuki sistim jaringan komputer yang menjadi targetnya. Tidak perduli apakah didalam jaringan tersebut sudah mempunyai sistem pengamannya atau belum[15].

Hal tersebut diperparah lagi dengan kenyataan bahwa banyak sekali situs-situs bawah tanah (underground sites) dalam Internet yang menawarkan informasi serta pengetahuan tentang bagaimana menembus sebuah sistim jaringan komputer (penetrated) sekaligus mengelabui sistem pengamanannya (security compromised). Informasi-informasi tersebut tersedia dalam bentuk kumpulan program, dokumentasi atau utiliti.Kumpulan informasi tersebut semakin memudahkan para cyber terrorist untuk melaksanakan niatnya terhadap target yang telah ditentukannya. Dengan memanfaatkan sistim informasi yang tersedia tersebut para cyberterrorist dapat menyampaikan "pesannya (messages)" ke seluruh dunia dengan cepat. Sudah berulangkali diadakan seminar, simposium serta diskusi-diskusi dengan topik utama mengenai pengamanan jaringan komputer.

6. Kesimpulan

Kejahatan dunia maya (*cyber crime)* merupakan fenomena sosial yang terjadi di ruang maya, sejatinya adalah kejahatan secara konvensional yang berpindah ruang di dalam dunia maya, namun esensinya sama yaitu melakukan tindak pidana kejahatan dengan penggunaan kemajuan teknologi adalah komputer dengan program internet

[15] Wisnubroto, AI.(2010), *Strategi Penanggulangan Kejahatan Telematika*. Atma Jaya, Yogyakarta

sebagai alat (tool) dalam melakukan tindak pidana kejahatan. Konsekuensi logis atass kemajuan teknologi menimbulkan kejahatan yang berbasis teknologi dalam penyalahgunaan komputer (computer misuse), yang banyak dikenal dengan istilah kejahatan dunia maya (*cyber crime).* Kejahatan dunia maya ini termasuk di dalamnya adalah kejahatan terorisme *(cyber terrorism).*

Tindak pidana terorisme menjadi perhatian dunia, karena sifatnya yang melakukan teror dengan menggunakan perangkat komputer *(computer related crime)* dalam melakukan aksi tindak pidana terorismenya tentunya dengan convergance teknologi memudahkan kejahatan terorisme dalam ruang maya bergerak leluasa disebabkan jangkauan sasaran dan objek yang dituju bersifat tanpa batas (*borderless).* Cyber terrorism dinyatakan sebagai kejahatan yang luar biasa (*extra ordinary crime*) dan semua negara menyoroti tindak kejahatan ini yang berdampak pada gangguan keamanan negara dan setiap orang yang menjadi warga negara tidak merasa aman dan tenang oleh aksi kejahatan teroris yang mulai berinvasi ke dalam ruang maya (*cyber space).* Kejahatan terorisme dikatakan extra ordinary crime itu karena sifat kejahatan teroris kini bergerak melakukan aksinya melampaui batas negara dan terorganisir (transnational organice crime).

Cyber crime adalah satu diantara perkembangan kejahatan berbasis teknologi yang membawa permasalahan di bidang hukum. Kejahatan di ruang dunia maya (cyber crime) dalam dunia virtual ini merupakan kejahatan modern yang bersifat kompleks, rumit dan tidak mengenal batas waktu/ruang (*borderless),* memerlukan penanganan hukum secara khusus lex specialis dalam menghadirkan perangkat hukum yang berkaitan dengan penegakan hukum dunia maya (*cyber law).*

Itu berarti perlunya dilakukan revisi terhadap Undang-Undang ITE agar dapat menyempurnakan penyelesaian permasalahan hukum dalam hal tindak pidana terhadap Informatika dan telematika, terkait penegakan hukum atas tindak pidana terorisme (*cyber terrorism)* dan kejahatan *cyber (cyber crime)* lainnya, yang banyak merugikan orang lain dan mengancam keamanan setiap orang dan keamanan negara secara luas.

REFERENSI

Abdul Hakim Garuda Nusantara, (2003), *Undang-Undang Pemberantasan Tindak Pidana Terorisme Dalam Perspektif Negara Hukum.* Bandung: Badan Pembinaan Hukum Nasional

Andi Hamzah, (1989), *Aspek-Aspek Pidana Di Bidang Komputer*, Jakarta: Ghalia

Andrew Michael Colarik, *Cyber Terrorism:Political and Economic Implications*, USA: Idea Group Publishing

Bhakti, A. S, (2016), *Deradikalisasi Dunia Maya, Mencegah Simbiosis Terorisme dan Media.* Jakarta: Daulat Press.

Golose, Petrus Reinhard, (2015), Invasi Terrorisme Ke Cyberspace. Jakarta: YPKIK

Josua Sitompul, (2012), *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*, Jakarta: Tatanusa, 2012.

Lukasz Jachowicz, *Cyberterrorism And Cyberhooliganism: How To Prevent And Fight International and Domestic*, paper presented at Collegium Civitas Foreign Policy of the United States of America, January 2003

Romli Atmasasmita, (2003), *Aspek Nasional Dan Global Pemberantasan Terorisme*. Jurnal Hukum Internasional, v2n3.

Widodo. (2010), *Sistem Pemidanaan Dalam Cyber Crime.* Yogyakarta: Laksbang Mediatama

Wisnubroto, AI. (2010), *Strategi Penanggulangan Kejahatan Telematika*. Yogyakarta: Atma Jaya

https://www.kompas.com/skola/read/2020/04/03/121500469/demokrasi-pancasila--pengertian-dan keunggulannya?page=all.

faizbmarwan/560d3e78349773ef0b6b5009/keterkaitan Antara demokrasi-dan-terorisme//page=all