ISSN 2656-4041 (Media Online)

ANTI TERORISME SIBER: UPAYA ANTISIPATIF PENANGGULANGAN TERORISME SIBER DI INDONESIA

Oleh:

Ardison Asri, Lasmauli Noverita Simarmata, Aria Caesar Kusuma Atmaja, Ario Wendra

Dosen Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma
Jl. Protokol Halim Perdanakusuma, Komplek Angkasa Halim Perdanakusuma, Jakarta 13610
Email: ardison@unsurya.ac.id

Abstrak

Terorisme siber atau disebut juga dengan *cyber terrorism* merupakan salah satu jenis kejahatan yang termasuk dalam kategori kejahatan dunia maya (*cyber crime*) disamping kejahatan dunia maya (*cyber crime*) lainnya. Lalu, bagaimana ciri-ciri dan bentuk-bentuk terorisme dunia maya sebagai salah satu bentuk kejahatan dunia maya (*cyber crime*) serta bagaimana upaya antisipasi anti terorisme dunia maya (*cyber terrorism*) di Indonesia. Untuk membahas hal tersebut, digunakan metode penelitian normatif. Bahan hukum dalam penelitian ini terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Metode pendekatan yang digunakan adalah pendekatan perundang-undangan, pendekatan kasus, dan pendekatan konseptual. Teknik pengumpulan data melalui studi dokumen atau studi kepustakaan. Analisis data yang digunakan adalah analisis kualitatif. Dari hasil penelitian, ditemukan bahwa terorisme dunia maya merupakan salah satu dimensi kejahatan kontemporer yang merupakan transformasi dari kejahatan teroris konvensional. Pemanfaatan jaringan internet oleh teroris dapat dengan mudah melakukan serangan dan mereka akan sulit untuk diidentifikasi. Pergeseran tindakan terorisme ini harus diikuti dengan pendekatan integral antara kebijakan penal dan non penal, dimana kebijakan pidana tidak hanya menggunakan sarana penal saja tetapi dapat juga menggunakan sarana non penal yaitu sarana di luar hukum pidana sebagai upaya preventif dalam upaya pencegahan tindak pidana terorisme dunia maya.

Kata kunci: Upaya Antisipatif, Siber, Terorisme Siber.

Abstract

Cyber terrorism or also called cyber terrorism is a type of crime that is included in the cybercrime category in addition to other cybercrimes. Then, what are the characteristics and forms of cyber terrorism as a form of cybercrime and what are the anticipatory anti-cyber terrorism efforts in Indonesia. To discuss this, normative research methods are used. The legal materials in this research consist of primary legal materials, secondary legal materials and tertiary legal materials. The approach methods used are the statutory approach, case approach and conceptual approach. Data collection techniques through document study or literature study. The data analysis used is qualitative analysis. From the research results, it was found that cyber terrorism is one dimension of contemporary crime which is a transformation of conventional terrorist crimes. The use of internet networks by terrorists can easily carry out attacks and they will be difficult to identify. This shift in acts of terrorism must be followed by an integral approach between penal and non-penal policies, where criminal policies do not only use penal means but can also use non-penal means, namely means outside criminal law as preventive measures in efforts to prevent criminal acts. cyber terrorism.

Keywords: *Anticipatory Efforts, Cyber, Cyber Terrorism.*

ISSN 2656-4041 (Media Online)

A. PENDAHULUAN

Indonesia dan seluruh dunia pada era ini telah terhubung oleh teknologi informasi dan komunikasi. Sistem telekomunikasi dan komputer dapat terhubung secara global (*have global reach*), baik mentransfer suara dan data digital yang melintasi batas-batas negara. Sistem tersebut juga menjadi penggerak untuk mendukung pengembangan infrastruktur ekonomi dan industry 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*) 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 ilmuan, pengguna umum melainkan juga dipakai oleh mata-mata dan teroris.[1]

Jaringan internet dimanfaatkan oleh pelaku terorisme untuk menunjang kegiatan teroris. Penggunaan internet oleh teroris dikenal dengan *terrorist use the internet*. Lebih lanjut, penggunaan internet oleh teroris atau sekolompok orang untuk melakukan kejahatan terorisme dikenal dengan istilah *cyber terrorism*. Dengan menggunakan jaringan internet, para teroris dapat dengan mudah melakukan serangan karena lewat jaringan internet meraka akan sulit untuk diidentifikasikan.[2]

Terorisme siber atau *cyber terrorism* merupakan salah satu dimensi dari kejahatan masa kini atau merupakan transformasi dari terorisme konvensional. Contoh nyata yang dapat kita lihat saat ini adalah organisasi radikal *Islamic State of Iraq and Syam/Syria* atau yang lebih dikenal dengan ISIS telah menggunakan alat teknologi dalam melakukan aksi kejahatan berkaitan dengan ideologi dan pencucian otak (*brain wash*) mengenai paham negara dan perekrutan. ISIS telah menggunakan jejaring media sosial melalui *Twitter*, *Facebook*, *YouTube*, dan lain sebagainya untuk merekrut anggota baru, alat propaganda, dan terus secara kuat mempublikasikan keberadaan kelompoknya sebagai kekuatan negara baru yang akan memimpin kekhalifahan di muka bumi, serta dengan berbagai cara melakukan aksi teror melalui dunia maya.[3]

Aksi teror melalui dunia maya inipun telah banyak terjadi diberbagai negara, tidak luput juga di Indonesia. Kasus yang terjadi pada Kedutaan Besar Sri Lanka di berbagai negara yang dibanjiri oleh hampir 800 *email* yang semuanya berisi tentang ancaman dari kelompok yang menamakan dirinya *Black Tigers*. Begitu pula di Cina, sekelompok *hacker* Cina mematikan satelit Cina. Sabotase internet yang terjadi di *Babha Atomic Research Centre*, India. Serangan dari gerakan *Eurasian Youth Movement* terhadap infrastruktur informasi di Estonia. *Cyber terrorism* juga terjadi di

[1] Zephirinus Jondong, Kebijakan Hukum Pidana Bagi Tindak Pidana *Cyber Terrorism* Dalam Rangka Pembentukan Hukum Positif di Indonesia, Jurnal Preferensi, Vol. 1, No. 2, 2020, hlm. 21-27.

[2] Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian* Cybercrime, (Jakarta: Rajagrafindo Persada, 2006), hlm. 21.

[3] kominfo.go.id, "ISIS Sebar Paham Radikal Melalui Media Digital", terdapat pada situs https://www.kominfo.go.id/content/detail/4523/isis-sebar-paham-radikal-melalui-media-digital/0/sorotan_media, diakses tanggal 25 Agutus 2024, pukul 20.15 Wib.

ISSN 2656-4041 (Media Online)

Eropa yang dilakukan oleh *Greek Security and Intrude*, dimana serangan dilakukan terhadap sistem komputer *European Organization for Nuclear Research* (pengembangan nuklir terbesar di dunia). Tahun 2016 muncul serangan virus *ransomware wannacry* terhadap beberapa rumah sakit di hampir 100 negara di seluruh dunia, termasuk Indonesia. Munculnya virus tersebut diduga akibat serangan yang menggunakan media internet untuk membuat sistem komputer dan peralatan teknologi rumah sakit menjadi lumpuh.[4]

Atas kasus-kasus tersebut di atas, artinya *cyber terrorism* telah terjadi dan ini tentu sangat berbahaya dan harus diwaspadai. Hal ini juga pernah disampaikan oleh almarhum Imam Samudra salah satu pelaku Bom Bali ketika masih hidup pada saat memberikan keterangan dalam proses penyelidikan, dimana Imam Samudra mengemukakan bahwa internet adalah alat yang terbaik untuk mencapai misinya. Pernyataan itu ia tuangkan dalam bukunya yang berjudul "Aku Melawan Teroris (*I Fight Terorists*)". Ia menyarankan kepada junior-juniornya untuk belajar internet sehingga terampil seperti *hacker*. Bagi mereka tujuan utamanya adalah untuk berbagi pengetahuan mengenai *hacking*, serta sebagai alat perlawanan politik.[5]

Maraknya kasus terorisme siber secara global maupun khusus di Indonesia membuat kejahatan terorisme ini menjadi semakin kompleks. Terorisme yang secara umum dimaknai sebagai serangan terkoordinasi yang bertujuan membangkitkan perasaan teror terhadap sekolompok masyarakat yang secara konvensional dalam menjalankan aksinya dilakukan seperti melakukan bom bunuh diri.[6] Sedangkan terorisme siber (*cyber terrorism*) merupakan konvergensi terorisme dan *cyberspace*.[7] Terorisme siber adalah serangan teroris yang menggunakan peralatan jaringan komputer (*cyberspace*) untuk mengganggu sistem infrastruktur negara (energi, transportasi, operasional pemerintah, dan sejenisnya) atau untuk mengintimidasi pemerintah atau sekolompok masyarakat sipil.[8]

Berdasarkan dari yang dikemukakan di atas, telah terjadi pergeseran atau evolusi aksi terorisme yang semula berupa serangan bersifat nyata/fisik bergeser pada serangan mayantara. *Cyber terrorism* diidentifikasikan sebagai serangan terhadap infrastruktur nasional yang kritis atau intimidasi terhadap warga sipil dan pegawai pemerintahan dengan menggunakan jaringan dan teknologi komputer. *Cyber terrorism* juga dianggap sebagai serangan yang melanggar hukum terhadap jaringan komputer, jaringan informasi yang tersimpan yang bertujuan untuk mengintimidasi pemerintah atau rakyatnya. Serangan tersebut

[4] Danang Enggartyasto dan Irwan Hafid, Kebijakan Hukum Pidana Terhadap Upaya Pemberantasan Terorisme Siber di Indonesia, Jurnal *Lex Renaissance*, Vol. 7, No. 1, 2022, hlm. 84-99.

[5] thejakartapost.com. "*Cyber Terrorism Creates Problems Real World"*, terdapat pada situs http://www.thejakartapost.com/news/2006/09/14/cyberterrorism-creates-problems-real-world.htm, diakses tanggal 25 Agustus 2024, pukul 20.15 Wib.

[6] Indriyanto Seno Adji, *Terorisme dan HAM Dalam Terorisme: Tragedi Umat Manusia*, (Jakarta: O.C. Kaligis & Associates, 2001), hlm. 17.

[7] Dwila Annisa Rizki Amalia, Kebijakan Hukum Pidana Dalam Upaya Penanggulangan *Cyber Terorism*, Jurnal Pembangunan Hukum Indonesia, Vol. 3, No. 2, 2021, hlm. 228-239.

[8] Zephirinus Jondong, *Loc. Cit*.

ISSN 2656-4041 (Media Online)

menghasilkan kekerasan terhadap individu, kelompok atau property pemerintah dan menimbulkan bahaya dan ketakutan. Sistem satelit, telekomunikasi, perbankan, pengendalian lintas udara, sistem navigasi alut, jaringan telekomunikasi, distribusi listrik, jaringan pertahanan dan keamanan termasuk sistem pengendalian *weapon of mass destruction* (WMD) termasuk bom nuklir, kesehatan, dan bentuk-bentuk fasilitas pelayanan public lainnya menjadi sasaran kejahatan terorisme.

Bertitik tolak dari uraian di atas, maka *cyber terrorism* atau disebut juga terorisme dunia maya merupakan salah satu jenis kejahatan yang masuk dalam kategori *cyber crime* disamping kejahatan-kejahatan siber lainnya. Lalu, bagaimana karakteristik dan bentuk *cyber terrorism* sebagai salah satu bentuk kejahatan siber (*cyber crime*) dan bagaimana upaya antisipatif anti terorisme siber di Indonesia.

B. METODE PENELITIAN

Metode penelitian yang digunakan adalah penelitian normatif, yang menurut Soejono Soekanto dan Sri Mamudji, pengertian penelitian normatif atau disebut juga penelitian hukum kepustakaan adalah penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder belaka.[9] Penelitian normatif ini difokuskan pada bahan yang digunakan di dalam penelitiannya. Bahan hukum yang diteliti di dalam penelitian normatif ini terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tertier.[10] Sementara metode pendekatan yang digunakan adalah metode pendekatan perundang-undangan (*statute approach*), pendekatan kasus (*case approach*), dan pendekatan konseptual (*conseptual approach*). Teknik pengumpulan data melalui studi dokumen atau studi kepustakaan. Analisis data yang digunakan adalah analisis kualitatif. Sedangkan metode analisis data yang digunakan bersifat deskriptif analitis yaitu analisis data yang digunakan adalah analisis kualitatif terhadap data sekunder. Deskriptif tersebut meliputi isi dan struktur hukum postif yaitu suatu kegiatan yang dilakukan peneliti untuk menentukan isi atau makna aturan hukum yang dijadikan rujukan dalam menyelesaikan permasalahan hukum yang menjadi objek kajian.[11]

C. HASIL DAN PEMBAHASAN

1. Terorisme Siber Merupakan Cyber Crime

Cyber crime atau ada yang menggunakan istilah *technological crime*, *high technology crime*, *high tech crime*, *internet crime*, *digital crime* yang semua istilah tersebut merupakan penggambaran kejahatan yang dilakukan dengan komputer atau teknologi informasi lainnya oleh orang-orang.[12] Begitu pula terminologi *cyber crime* memiliki pengertian yang berbeda-beda pula menurut beberapa literatur dan ahli. Menurut Thomas and Loader berpendapat bahwa *cybercrime* adalah aktivitas yang menggunakan media komputer yang ilegal atau

[9] Soejono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif (Suatu Tinjauan Singkat)*, (Jakarta: Rajagrafindo Persada, 2014), hlm. 14.

[10] Sunaryati Hartono, *Penelitian Hukum di Indonesia Pada Akhir Abad Ke-20*, Cet. 2, (Bandung: Alumni, 2006), hlm. 16.

[11] Zainuddin Ali, *Metode Penelitian Hukum*, Cet. 3. (Jakarta: Sinar Grafika, 2011), hlm. 107.

[12] Ardison Asri, *Tindak Pidana Khusus*, (Sukabumi: CV Jejak, 2022), hlm. 120.

ISSN 2656-4041 (Media Online)

dianggap ilegal oleh pihak-pihak tertentu yang dapat dilakukan melalui jaringan elektronik global.[13] Ada juga yang mendefinisikan *cyber crime* itu sebagai suatu perbuatan yang melanggar hukum karena tindakan yang dilakukan dapat mengancam serta merusak infrastruktur teknologi informasi suatu negara, seperti halnya akses ilegal atau tanpa seizin orang berwenang, tindakan maupun percobaan mengakses baik sebagian maupun keseluruhan bagian sistem komputer yang mana pelaku tidak mempunyai hak untuk melakukan pengaksesan terhadapnya. Pada dasarnya *cyber crime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi serta sistem komunikasi yang merupakan sarana untuk penyampaian atau pertukaran informasi kepada pihak lainnya.[14]

Sementara kebijakan hukum pidana Indonesia belum ada yang menjelaskan mengenai pengertian *cyber crime*. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik[15] yang telah mengalami beberapa kali perubahan yakni Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik[16] dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik[17], bila dilihat dari materinya mengatur 2 (dua) hal secara garis besar, yaitu: pertama, pengaturan tentang informasi dan transaksi elektronik; dan kedua, pengaturan tentang perbuatan-perbuatan yang dilarang (*cyber crime*).[18]

Pengaturan hal kedua di atas dalam Undang-undang tentang Informasi dan Transaksi Elektronik tersebut mengacu pada *EU Convention on Cybercrime, 2001* yang merupakan instrumen internasional yang digunakan oleh banyak negara.[19] Dalam *background paper* untuk lokakarya Kongres Perserikatan Bangsa-Bangsa (PBB) X/2000 di Wina Austria, istilah *cyber crime* dibagi 2 (dua) kategori. Pertama, *cyber crime* dalam arti sempit (*in a narrow sense*) yang disebut *computer crime*. Kedua, *cyber crime* dalam arti luas (*in a broader sense*) yang disebut *computer related crime*. Selangkapnya dijelaskan sebagai berikut:

---

[13] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber*, (Bandung: Refika Pratama, 2012), hlm. 92.

[14] Dikdik M. Arief Mansur dan Elisataris Ghultom, *Cyber Law – Aspek Hukum Teknologi Informasi*, (Bandung: Refika Aditama, 2005), hlm. 10.

[15] Indonesia, *Undang-Undang Republik Indonesia tentang Informasi dan Transaksi Elektronik*, Undang-Undang Republik Indonesia Nomor 11 Tahun 2008, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

[16] Indonesia, *Undang-Undang Republik Indonesia tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*, Undang-Undang Republik Indonesia Nomor 19 Tahun 2016, Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

[17] Indonesia, *Undang-Undang Republik Indonesia tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*, Undang-Undang Republik Indonesia Nomor 1 Tahun 2024, Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905.

[18] Putu Sekarwangi Saraswati dan I Nengah Susrama, Pengaturan *Cyber Terrorism* Ditinjau Dari Perspektif *Organizational Transnational Crime*, Jurnal Penelitian Pendidikan Indonesia, Vol. 10, No. 2, 2024, hlm. 308-316.

[19] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*, (Jakarta: Tatanusa, 2012), hlm. 38.

ISSN 2656-4041 (Media Online)

1. *Cyber crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed by them*.
2. *Cyber crime in broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possess pion, offering, or distributing information by means of a computer system or network*.[20]

Berdasarkan pengertian-pengertian kejahatan siber (*cyber crime*) di atas, dapat dilihat karakteristik dari *cyber crime* tersebut adalah sebagai berikut:

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis yang terjadi dalam ruang atau wilayah siber (*cyberspace*);
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet;
3. Perbuatan tersebut mengakibatkan kerugian materil maupun immaterial (waktu, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional;
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya;
5. Perbuatan tersebut sering dilakukan secara trannasional atau melintasi batas negara.

Sedangkan menurut Golose dalam kejahatan dunia maya baik korban maupun pelaku tidak saling berhadapan langsung dalam tempat kejadian perkara. Dalam beberapa kasus baik korban maupun pelaku dapat berada pada negara yang berbeda. Hal tersebut menggambarkan bahwa kejahatan dunia maya merupakan salah satu bentuk kejahatan lintas negara (*transnastional crime*) dan tak berbatas (*borderless*), tanpa kekerasan (*non violence*), tidak ada kontak fisik (*no physically contact*) dan tanpa nama (*anonimity*).[21]

Bila ditinjau dari pengertian dan karakteristik *cyber crime*, tentu tidak bisa kita menyebut bahwa setiap serangan pada sistem elektronik sebagai kejahatan terorisme siber (*cyber terrorism*) atau meskipun suatu kejahatan itu dilakukan menggunakan teknologi informatika. Barry Collin, *researcher di Institute form Security and Intelligence in California* menciptakan istilah *cyber terrorism* pada tahun 1980-an. Konsep ini terdiri dari 2 (dua) elemen penting, yaitu elemen dunia maya dan terorisme.[22] Artinya, dalam kejahatan *cyber terrorism*, selain kejahatan itu dilakukan dengan menggunakan alat teknologi juga harus diikuti dengan unsur atau adanya elemen terorisme.

[20] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Penanggulangan Kajahatan*, (Jakarta: Kencana Predana Media Group, 2007), hlm. 24.

[21] Petrus Reinhard Golose, Perkembangan *Cyber Crime* dan Upaya Penanggulangannya di Indonesia Oleh Polri, Buletin Hukum Perbankan dan Kebanksentralan, Vol. 4, No. 2, 2006, hlm. 34.

[22] Barry Collin, "Cyber Terrorism is Real – is it? Introduction in the 1980's Barry Collin", terdapat pada situs http://www.intelligence-andinvestigations.com/media/uploads/62_Cyber terrorism%20- %20Nicholas%20Bradley.pdf, diakses tanggal 28 Agustus 2024, pukul 21.30 Wib.

ISSN 2656-4041 (Media Online)

Istilah terorisme berasal dari bahasa Inggris yaitu *terrorism*, yang diambil dari istilah bahasa Latin yakni *terrere* yang berarti menyebabkan ketakutan. Sehingga kata teror berarti menakut-nakuti.[23] 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.[24]

Sementara pengertian terorisme menurut Undang-Undang Republik Indonesia Nomor 5 Tahun 2018 tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang pada Pasal 1 angka 2 dijelaskan bahwa terorisme adalah perbuatan yang menggunakan kekerasan atau ancaman kekerasan yang menimbulkan suasana terror atau rasa takut secara meluas yang dapat menimbulkan korban yang bersifat massal, dan/atau menimbulkan kerusakan atau kehancuran terhadap objek vital yang strategis, lingkungan hidup, fasilitas publik, atau fasilitas internasional dengan motif ideologi, politik, atau gangguan keamanan.

Dengan demikian, kejahatan *cyber terrorism* merupakan suatu kejahatan siber yang didalamnya terdapat unsur-unsur tindak pidana terorisme. Untuk dapat memahami lebih lanjut dapat dikemukakan karakteristik dan bentuk *cyber terrorism* sebagai salah satu bentuk kejahatan siber (*cyber crime*) adalah sebagai berikut:

1. *Actors* (Pelaku)
   Bahwa pelaku *cyber terrorism* merupakan para teroris. Pelaku melakukan kegiatan teror dengan menggunakan komputer yang terhubung jaringan internet sebagai alat dan sarana dalam melakukan aksi kekerasan, intimidasi, dan lain sebagainya.
2. *Tools* (Alat)
   Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet. Adapun tujuannya adalah melakukan serangan secara massif untuk penetrasian terhadap jaringan keamanan komputer dan menghilangkannya atau mematikan fungsi-fungsi pentingnya.
3. *Targets* (Sasaran)
   Sistem informasi merupakan kebutuhan dasar bagi suatu negara untuk pelayanan bagi kepentingan publik. Hal inilah yang menjadi sasaran atau target *cyber terrorism* seperti *government*, *public health*, *emergency services*, *information and telecommunication*, *energy*, *transportation*, *banking and finance*, dan fasilitas vital lainnya.
4. Motif
   Adapun motif pelaku *cyber terrorism* adalah motif

[23] Asep Syamsul M Romli, *Demologi Islam: Upaya Barat Membasmi Kekuatan Islam*, (Jakarta: Gema Insani, 2003), hlm. 39.

[24] I Gede Pasek Eka Wisanjaya, *Pengaturan Tentang Terorisme Dalam Hukum Internasional dan Hukum Nasional*, (Bali: Fakultas Hukum Universitas Udayana, 2016), hlm. 10.

ISSN 2656-4041 (Media Online)

ideologi, politik, atau gangguan keamanan yang semuanya bertujuan untuk menimbulkan suasana terror atau rasa takut dan/atau menimbulkan kerusakan atau kehancuran terhadap objek vital yang strategis.

2. Upaya Antisipatif Penanggulangan Terorisme Siber di Indonesia

Upaya pemberantasan terorisme oleh negara-negara di dunia ternyata memunculkan kegiatan terorisme dengan strategi dan taktik baru. Salah satunya adalah pergeseran aksi terorisme dari aksi nyata atau fisik beralih aksi terorisme melalui dunia maya. Pergeseran aksi terorisme inilah yang harus diikuti dengan upaya penanggulangan tindak pidana teroris melalui dunia maya melalui pendekatan teknologi (*techno prevention*) disamping melalui kebijakan kriminalisasi melalui pembentukan undang-undang.

Pendekatan yang semacam ini merupakan pendekatan integral antara kebijakan penal dan non-penal, sebagaimana yang dikemukakan oleh Muladi dan Barda Nawawi Arif bahwa kebijakan kriminal tidak hanya menggunakan sarana penal tetapi dapat juga menggunakan sarana-sarana non-penal yakni sarana di luar hukum pidana sebagai langkah preventif dalam upaya pencegahan tindak pidana *cyber terrorism*.[25] Oleh karena itu, upaya anti *cyber terrorism* di Indonesia dapat dilakukan melalui:

1. Upaya Penal

   Adapun upaya penal dalam penanggulangan tindak pidana terorisme siber ini dapat dilakukan melalui:

   a. Positifisasi perbuatan tindak pidana terorisme siber (*cyber terrorism*) melalui Undang-undang Informasi dan Transaksi Elektronik

      Indonesia sudah sejak jauh hari mengatur tentang tindak pidana terorisme dengan Undang-Undang Republik Indonesia Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang *jo.* Undang-Undang Republik Indonesia Nomor 5 Tahun 2018 tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang, namun dianggap belum cukup untuk mencegah berbagai kegiatan terorisme yang semakin berkembang seperti *cyber terrorism*.

      Sebagaimana yang telah dibahas pada bagian sebelumnya, bahwasanya tindak pidana *cyber terrorism* merupakan bagian/jenis dari kejahatan *cyber crime*. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah mengalami beberapa kali perubahan yakni Undang-

[25] Muladi dan Barda Nawawi Arief, *Teori-teori dan Kebijakan Pidana*, (Bandung: Alumni, 2010), hlm. 158.

ISSN 2656-4041 (Media Online)

Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, disamping mengatur tentang pengaturan informasi dan transaksi elektronik juga mengatur tentang pengaturan kejahatan-kejahatan yang berbasis teknologi (*cyber crime*). Ketentuan pidana dalam Undang-undang tentang Informasi dan Transaksi Elektronik terdapat dalam Bab XI Pasal 45 sampai dengan Pasal 52. Ketentuan pasal-pasal pada Bab XI diidentifikasikan mengenai beberapa perbuatan tindak pidana yang dapat dikaitkan dengan tindak pidana *cyber terrorism*. Pasal 30 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 terkait dengan aksi kejahatan *cyber terrorism* berbentuk pengaksesan yang tidak sah ke sistem dan layanan komputer atau yang lebih dikenal sebagai *illegal acces*. Sedangkan ketentuan Pasal 31 terkait tindak pidana intersepsi dan penyadapan atau yang lebih dikenal sebagai *illegal interception*. Pasal 32 terkait tindak pidana gangguan data atau yang lebih dikenal sebagai *data interference*. Pasal 33 terkait tindak pidana gangguan sistem atau yang disebut sebagai *system interference*.

Dengan demikian, perspektif Undang-undang tentang Informasi dan Transaksi Elektronik yang telah ditetapkan oleh Indonesia adalah menekakan pada aspek penggunaan dan keamanan sistem informasi elektronik dan dokumen elektronik dan penyalahgunaan dibidang teknologi dan transaksi elektronik yang dilakukan termasuk para pelaku *cyber terrorism*.

b. Tindak pidana terorisme siber (*cyber terrorism*) dalam Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-undang Hukum Pidana

Meskipun Indonesia telah memiliki aturan mengenai kejahatan siber namun usaha terhadap pembaharuan hukum pidana (*penal reform*) masih terus dilakukan karena merupakan bagian dari kebijakan atau politik hukum pidana (*penal policy*). Pembaharuan hukum pidana secara umum mempunyai makna sebagai suatu upaya untuk melakukan reorientasi dan reformasi hukum pidana. Misalnya di dalam Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-undang Hukum Pidana telah diatur mengenai kejahatan di bidang teknologi informasi sehingga sebagai bentuk upaya penanggulangan kejahatan *cyber terrorism*.

Hal tersebut di atas, dapat dilihat dalam ketentuan Buku Pertama Undang-Undang Republik Indonesia Nomor 1 Tahun 2023, Pasal 4, Pasal 5,

ISSN 2656-4041 (Media Online)

Pasal 147, Pasal 148, Pasal 157, Pasal 158, Pasal 164, Pasal 167, Pasal 169, Pasal 170, Pasal 171. Disamping itu di dalam Buku Kedua Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 juga dilakukan perubahan perumusan delik atau penambahan delik-delik baru yang berkaitan dengan kemajuan teknologi dengan harapan dapar menjaring kasus-kasus *cyber terrorism*. Contohnya pada ketentuan Bab VIII tentang Tindak Pidana yang Membahayakan Keamanan Umum Bagi Orang, Kesehatan, dan Barang pada Pasal 332, Pasal 333, Pasal 334, Pasal 335.

2. Upaya Non-Penal

Adapun upaya penal dalam penanggulangan tindak pidana terorisme siber ini dapat dilakukan melalui:

a. Pendekatan Teknologi (*Techno Prevention*)

Cyber terrorism merupakan jenis kejahatan yang terkait erat dengan teroris yang menggunakan teknologi maju sebagai sarana dan sasaran serangan teroris. Maka tidak salah dalam menghadapi model kejahatan baru itu harus mengedepankan pendekatan teknologi. Hal tersebut dapat dilakukan dengan cara membatasi akses, memasang proteksi atau *security cyber*, sistem pemantauan serangan, back up data secara rutin, dan penggunaan enkripsi untuk meningkatkan keamanan terhadap sistem komputer.[26]

b. Kerjasama Internasional

Mengingat karakteristik *cyber terrorism* tidak mengenal batas-batas negara, maka dalam upaya penanggulangannya memerlukan suatu koordinasi dan kerjasama antar negara. Disamping itu, *cyber terrorism* tidak saja menjadi masalah yang bersifat nasional tetapi telah menjadi masalah internasional, sehingga kejahatan ini telah menjadi perhatian internasional.

Kongres Perserikatan Bangsa-Bangsa (PBB) ke-8 di Havana, Kongres X di Wina, Kongres XI di Bangkok berbicara tentang *The Prevention of Crime and the Treatment of Offender*. Dalam Kongres PBB X dinyatakan bahwa negara-negara anggota harus berusaha melakukan harmonisasi ketentuan-ketentuan yang berhubungan dengan kriminalisasi, pembuktian, dan prosedur (*States should seek harmonization of relevan provision on criminalization, evidence, and procedure*). Dua puluh satu negara dan negara-negara Uni Eropa yang telah secara serius mengintegrasikan regulasi yang terkait dengan pemanfaatan teknologi informasi ke dalam instrumen hukum positif (*existing law*) nasionalnya. *The Convention on Cybercrime is intended to improve law enforcement's*

[26] Barda Nawawi Arief, *Sari Kuliah Perbandingan Hukum Pidana*, (Jakarta: Rajagrafindo Persada, 2002), hlm. 254-255.

ISSN 2656-4041 (Media Online)

ability to react to cybercrime (Council of Europe, 2001). It seeks to achieve this by: (1) harmonising the domestic criminal substantive law . . . in the area of cybercrime; (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences . . .; and (3) setting up a fast and effective regime of international co-operation.

Selain upaya-upaya yang dilakukan oleh PBB dalam menjalin kerjasama internasional guna penanggulangan *cyber terrorism* muncul juga beberapa organisasi yang berinisiatif untuk membuat lembaga-lembaga yang bersifat global untuk melawan *cyber crime* khususnya *cyber terrorism*, seperti *International Services on Discovery and Recovery of Electronic and Internet Evidence* (IOCE), *GECD Initiatives, Efforts of G-7 and G-8 Groups*.

Tidak saja di tingkat internasional, upaya penanggulangan *cyber terrorism* inipun telah diupayakan pada tingkat regional, seperti *ASEAN Convention on Counter Terrorism*. Konvensi itu oleh Indonesia telah diratifikasi melalui Undang-Undang Republik Indonesia Nomor 5 Tahun 2012 tentang Pengesahan *ASEAN Convention on Counter Terrorism*.[27]

c. Program Deradikalisasi Dunia Maya

Pemerintah harus tegas dalam mengatasi tindak pidana terorisme siber ini. Bila memang ada terdapat program penyebaran paham terorisme, maka pemerintah harus segera memblokir situs tersebut. Selain itu, pemerintah harus punya tindakan preventif guna meminimalisir gerakan terorisme siber semakin menjamur. Hal tersebut dapat diupayakan melalui pengenalan komputer kepada masyarakat terkait fungsi dan penggunaannya agar tidak disalahgunakan serta pengenalan penggunaan teknologi yang baik melalui kurikulum dunia pendidikan khususnya kepada generasi muda agar internet tidak digunakan untuk kegiatan yang tidak baik.

3. PENUTUP

Kesimpulan

Terorisme siber atau *cyber terrorism* merupakan salah satu dimensi dari kejahatan masa kini yang merupakan transformasi dari kejahatan terorisme konvensional. *Cyber terrorism* pada konsep ini terdiri dari 2 (dua) elemen penting, yaitu elemen dunia maya dan terorisme. Artinya, dalam kejahatan *cyber terrorism*, selain kejahatan itu dilakukan dengan menggunakan alat teknologi juga diikuti dengan unsur atau adanya elemen terorisme. Penggunaan jaringan internet oleh para teroris dapat dengan mudah melakukan

[27] Alfira N Samad, *Analisis Instrumen Cyber Terrorism Dalam Kerangka Sistem Hukum Internasional*, (Makassar: Universitas Hasanuddin, 2014), hlm. 4.

ISSN 2656-4041 (Media Online)

serangan dan meraka akan sulit untuk diidentifikasikan.

Pergeseran aksi terorisme inilah yang harus diikuti dengan pendekatan integral antara kebijakan penal dan non-penal, dimana kebijakan kriminal tidak hanya menggunakan sarana penal tetapi dapat juga menggunakan sarana-sarana non-penal yakni sarana di luar hukum pidana sebagai langkah preventif dalam upaya pencegahan tindak pidana *cyber terrorism*.

Daftar Pustaka

Buku

Adji, Indriyanto Seno. 2001. Terorisme dan HAM Dalam Terorisme: Tragedi Umat Manusia. O.C. Kaligis & Associates. Jakarta.

Ali, Zainuddin. 2011. *Metode Penelitian Hukum*. Cet. 3. Sinar Grafika. Jakarta.

Arief, Barda Nawawi. 2002. *Sari Kuliah Perbandingan Hukum Pidana*. Raja Grafindo Persada. Jakarta.

----------. 2006. *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime*. Rajagrafindo Persada. Jakarta.

----------. 2007. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana Dalam Penanggulangan Kajahatan*. Kencana Predana Media Group. Jakarta.

Asri, Ardison. 2022. *Tindak Pidana Khusus*. CV Jejak. Sukabumi.

Hartono, Sunaryati. 2006. *Penelitian Hukum di Indonesia Pada Akhir Abad Ke-20*, Cet. 2. Alumni. Bandung.

Mansur, Dikdik M. Arief. dan Elisataris Ghultom. 2005. *Cyber Law – Aspek Hukum Teknologi Informasi*. Refika Aditama. Bandung.

Muladi. dan Barda Nawawi Arief. 2010. *Teori-teori dan Kebijakan Pidana*. Alumni. Bandung.

Romli, Asep Syamsul M. 2003. *Demologi Islam: Upaya Barat Membasmi Kekuatan Islam*. Gema Insani. Jakarta.

Samad, Alfira N. 2014. *Analisis Instrumen Cyber Terrorims Dalam Kerangka Sistem Hukum Internasional*. Universitas Hasanuddin. Makassar.

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

Soekanto, Soejono. dan Sri Mamudji. 2014. *Penelitian Hukum Normatif (Suatu Tinjauan Singkat)*. Rajagrafindo Persada. Jakarta.

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

Jurnal dan Makalah

Amalia, Dwila Annisa Rizki. (2021). Kebijakan Hukum Pidana Dalam Upaya Penanggulangan *Cyber Terrorism*. Jurnal Pembangunan Hukum Indonesia. 3 (2): 228-239.

Enggartyasto, Danang dan Irwan Hafid. (2022). Kebijakan Hukum Pidana Terhadap Upaya Pemberantasan Terorisme Siber di Indonesia. Jurnal Lex Renaissance. 7 (1): 84-99.

Golose, Petrus Reinhard. 2006. Perkembangan *Cyber Crime* dan Upaya Penanggulangannya di Indonesia Oleh Polri. Buletin Hukum Perbankan dan Kebanksentralan. 4 (2): 34.

Jondong, Zephirinus. (2020). Kebijakan Hukum Pidana Bagi Tindak Pidana *Cyber Terrorism* Dalam Rangka Pembentukan Hukum Positif di Indonesia. Jurnal Preferensi. 1 (2): 21-27.

Saraswati, Putu Sekarwangi dan I Nengah Susrama. (2024). Pengaturan *Cyber*

ISSN 2656-4041 (Media Online)

Terrorism Ditinjau Dari Perspektif *Organizational Transnational Crime*. Jurnal Penelitian Pendidikan Indonesia. 10 (2): 308-316.

Peraturan Perundang-undangan

Indonesia. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

----------. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251. Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

----------. Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1. Tambahan Lembaran Negara Republik Indonesia Nomor 6905.

----------. Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-undang Hukum Pidana. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1. Tambahan Lembaran Negara Republik Indonesia Nomor 6842.

Internet

Collin, Barry. Cyber Terrorism is Real – is it? Introduction in the 1980's Barry Collin. http://www.intelligence-andinvestigations.com/media/uploads/62_Cyber terrorism%20-%20Nicholas%20Bradley.pdf. Diakses tanggal 28 Agustus 2024. Pukul 21.30 Wib.

kominfo.go.id. "ISIS Sebar Paham Radikal Melalui Media Digital". https://www.kominfo.go.id/content/detail/4523/isis-sebar-paham-radikal-melalui-media-digital/0/sorotan_media. Diakses tanggal 25 Agutus 2024. Pukul 20.15 Wib.

thejakartapost.com. "*Cyber Terrorism Creates Problems Real World"*. http://www.thejakartapost.com/news/2006/09/14/cyberterrorism-creates-problems-real-world.htm. Diakses tanggal 25 Agustus 2024. Pukul 20.15 Wib.