KEBIJAKAN HUKUM PIDANA BERDASARKAN UNDANG-UNDANG NOMOR 5 TAHUN 2018 MENANGGULANGI CYBERTERRORISM DI INDONESIA

Jem Forad Markoni Ginting
Fakultas Hukum, Universitas Dirgantara Marsekal Suryadarma, Indonesia

Abstract

Cyberterrorism attacks anything connected to the internet, especially crucial government objects, which can disrupt its operations and can result in greater casualties than conventional terrorism. Therefore, it is very interesting and important to learn more about how Indonesian criminal law policy handles cyberterrorism crimes based on Law Number 5 of 2018 and future criminal law policy efforts. To solve this problem, normative juridical legal research was carried out using statutory and conceptual regulatory approaches. Data collected from primary, secondary and tertiary legal sources was then analyzed using qualitative data analysis methods. The research results show that the criminalized clauses in the Law on the Eradication of Criminal Acts of Terrorism appear to criminalize acts related to internet misuse, which is a type of cyber terrorism crime. Due to the importance of regulations regarding cyberterrorism as part or type of cybercrime that utilizes internet technology, regulations regarding the internet must be moved.
Keywords: Cyberterrorism, Criminal Law Policy, Regulation

Cyberterrorism menyerang apa saja yang terhubung ke internet, terutama objek penting milik pemerintah, yang dapat mengganggu operasinya dan bahkan dapat mengakibatkan korban yang lebih besar daripada terorrisme konvensional. Oleh karena itu, sangat menarik dan penting untuk mempelajari lebih lanjut tentang bagaimana kebijakan hukum pidana Indonesia menangani tindak pidana cyber terrorism berdasarkan Undang-undang nomor 5 tahun 2018 dan upaya kebijakan hukum pidana yang akan datang. Untuk menyelesaikan masalah tersebut, dilakukan penelitian hukum yuridis normatif yang menggunakan pendekatan peraturan perundang-undangan dan konseptual. Data yang dikumpulkan dari sumber hukum primer, sekunder, dan tertier kemudian dianalisis menggunakan metode analisis data kualitatif. Hasil penelitian menunjukkan bahwa klausul-klausul yang dikriminalisasi dalam Undang-Undang Pemberantasan Tindak Pidana Terrorisme tersebut tampaknya mekriminalisasi perbuatan yang berkaitan dengan penyalahgunaan internet, yang merupakan jenis tindak pidana cyber terrorism. Karena pentingnya pengaturan mengenai cyber terrorism sebagai bagian atau jenis tindak pidana cyber yang memanfaatkan teknologi internet, pengaturan mengenai internet harus digerakkan.
Keywords: Cyberterrorism, Kebijakan Hukum Pidana, Regulasi

PENDAHULUAN

Perilaku masyarakat dan peradaban manusia telah berubah karena teknologi informasi dan komunikasi. Selain itu, kemajuan teknologi informasi telah menyebabkan perubahan sosial yang sangat cepat dan tanpa batas. Teknologi informasi sekarang menjadi pedang bermata dua: selain membantu kesejahteraan, kemajuan, dan peradaban manusia, juga menjadi alat untuk perbuatan melawan hukum.[1]

Dengan menggunakan teknologi internet, banyak masalah yang kompleks dapat diselesaikan dengan efektif dan efisien. Dengan kemajuan teknologi ini, orang mungkin cenderung melakukan hal-hal yang bertentangan dengan etika sosial. Dunia maya, dunia tanpa batas, atau realitas virtual—yang dikenal sebagai virtual reality—telah diciptakan melalui penggunaan teknologi internet, yang telah menghasilkan masyarakat dunia baru yang tidak lagi dibatasi oleh batas-batas wilayah negara yang dahulunya sangat penting. Dan ini disebut sebagai Bordeless World.[2]

Perkembangan teknologi informasi dan komunikasi memiliki banyak manfaat, tetapi ada juga efek negatifnya. Kriminalitas yang dilakukan dengan menggunakan teknologi ini mulai berjamur. Berkembangnya kriminalitas kuantitatif dan kualitatif menunjukkan dampak negatif dari perubahan pola perilaku pada era kehidupan global ini. Berbagai jenis kejahatan kini mulai muncul dengan dimensi baru, seperti penyalahgunaan komputer, kejahatan perbankan, dan lain sebagainya, yang semakin sulit untuk ditangani.[3]

Cyberspace adalah tempat masyarakat sedang membangun kebudayaan baru[4]. Manusia dapat "hidup" dalam dunia lain melalui cyberspace. Dunia yang memiliki kemampuan untuk mengambil alih dan menggantikan apa yang ada saat ini, yang lebih menggembirakan dari kesenangan yang ada, lebih menakjubkan dari fantasi yang ada, dan lebih menarik dari keghairahan yang ada.

Perkembangan dan kemajuan dalam teknologi informasi dan telekomunikasi telah menghasilkan jenis kejahatan baru yang dikenal sebagai cyberspace crime.[5] Ini adalah

---

[1] Ahmad M. Ramli, *Cyber Law dan HAKI Dalam Sistem Hukum di Indonesia*, (Bandung: Abacus, 2006), hlm. 1.

[2] Agus Raharjo, *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung: Citra Aditya Bahkti, 2002), hlm. 5.

[3] Kata Pengantar Prof. DR. Barda Nanawi Arief, SH., *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer*, Aloysius Wisnubroto, (Yogyakarta: Universitas Atma Jaya, 1999).

[4] Abdul Wahid, *Kejahatan Mayantara*, (Bandung: Refika Aditama, 2005), hlm. 32.

[5] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, (Bandung: Citra Aditya Bhakti, 2003), hlm. 255.

kejahatan yang terkait dengan aplikasi internet dan dikenal sebagai cybercrime. Masalah cyber terrorism adalah salah satu masalah yang sangat meresahkan dan mendapat perhatian nasional maupun internasional. Jenis cyber terrorism ini sering didefinisikan sebagai kejahatan terorisme yang menggunakan sarana teknologi dan informasi, elektronik. Cyber sabotage dan exortion adalah istilah lain untuk cyber terrorism. Jenis pelanggaran ini dilakukan dengan mengganggu, merusak, atau menghancurkan data, program komputer, atau sistem jaringan komputer yang terhubung ke internet.

Tidak adanya undang-undang yang mengatur tindak pidana cyber terrorism dalam transaksi elektronik di Indonesia menimbulkan ketidakpastian hukum karena apabila tindak pidana ini terjadi di Indonesia, banyak yang mempertanyakan dasar hukum apa yang harus digunakan untuk menjerat tindak pidana tersebut. Menurut ayat pertama Pasal 1 Kitab Undang-undang Hukum Pidana (KUHP), "Suatu perbuatan tidak dapat dipidana, kecuali berdasarkan ketentuan perundang-undangan yang telah ada."[6]

Pasal diatas disebut sebagai asas legalitas, juga dikenal sebagai "tidak ada delik, tidak ada pidana tanpa peraturan lebih dahulu," mengatakan bahwa jika seseorang ingin melakukan sesuatu yang salah, harus ada hukum yang mengaturnya. Jika tidak ada, perbuatan tersebut tidak dapat dianggap melanggar hukum sehingga tidak dapat dipidana.

Dengan demikian, apabila terjadi tindak pidana cyber terrorism yang berkaitan dengan transaksi elektronik, rumusan delik yang ada dalam 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[7] 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[8] dan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan

[6] Indonesia, Kitab-Undang-undang Hukum Pidana (KUHP), Pasal 1 ayat (1).
[7] Indonesia, *Undang-Undang Republik Indonesia Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-Undang*, Undang-Undang Nomor 15 Tahun 2003, Lembaran Negara Republik Indonesia Tahun 2003 Nomor 45, Tambahan Lembaran Negara Republik Indonesia Nomor 4284.
[8] Indonesia, *Undang-Undang Republik Indonesia 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*, Undang-Undang Nomor 5 Tahun 2018, Lembaran Negara Republik Indonesia Tahun 2018 Nomor 92, Tambahan Lembaran Negara Republik Indonesia Nomor 6216.

Transaksi Elektronik[9] jo. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.[10] Karena cakupan dan pengaturan dunia maya yang begitu luas, hal ini dianggap tidak dapat menjerat pelaku tindak pidana teroris di dunia maya.

Tujuan utama dari penelitian ini adalah sebagai berikut: untuk mempelajari dan menganalisis undang-undang pidana yang berlaku di Indonesia untuk menangani tindak pidana cyber terrorism berdasarkan Undang-undang nomor 5 tahun 2018; dan untuk mempelajari dan menganalisis undang-undang pidana yang akan datang untuk menangani tindak pidana cyber terrorism.

METODE PENELITIAN

Penelitian hukum yuridis normatif, juga dikenal sebagai penelitian hukum doktrinal, adalah jenis penelitian ini. Kajian hukum "doktrinal" atau "normatif" mengkaji, mempertahankan, dan mengembangkan konstruksi hukum positif melalui penggunaan logika.[11] Penelitian hukum doktrinal adalah penelitian berbasis kepustakaan, yang fokusnya adalah analisis bahan hukum primer dan bahan hukum sekunder.[12] Penulis menggunakan pendekatan perundang-undangan (statute approach), pendekatan kasus (case approach), dan pendekatan konseptual untuk menulis skripsi ini.

Penelitian ini menggunakan metode penelitian kepustakaan untuk mengumpulkan data. Penelitian ini menggunakan alat pengumpulan data seperti studi dokumen, studi pustaka, atau penelitian kepustakaan untuk mendapatkan data sekunder. Menurut Abdul Rahman Sholeh, penelitian kepustakaan adalah penelitian yang menggunakan metode untuk mendapatkan data informasi dengan menggunakan fasilitas yang ada di perpustakaan, seperti buku, majalah, dokumen, dan catatan sejarah.[13] Penelitian ini menggunakan pendekatan kualitatif, yang berarti menyusunnya secara sistematis dan menghubungkan satu sama lain terkait dengan masalah

---

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

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

[11] Saefullah Wiradipradja, *Penuntun Praktis Metode Penelitian dan Penulisan Karya Ilmiah Hukum,* Cet. 2, (Bandung: Keni Media, 2015), hlm. 5.

[12] Dyah Ochtorina Susanti & A'an Efendi, *Penelitian Hukum (Legal Research),* Cet. 1, (Jakarta: Sinar Grafika, 2014), hlm. 11.

[13] Abdul Rahman Sholeh, *Pendidikan Agama dan Pengembangn untuk Bangsa*, (Jakarta: Raja Grafindo Persada, 2005), hlm. 63.

yang diteliti. Penelitian ini juga mempertimbangkan struktur perundang-undangan dan keyakinan hukum, serta perundang-undangan yang berlaku yang dilaksanakan oleh penegak hukum.[14]

HASIL DAN PEMBAHASAN

A. Kebijakan Hukum Pidana Terkait Penanggulangan Tindak Pidana Cyber Terrorism di Indonesia Berdasarkan Undang-undang Nomor 5 tahun 2018

Pertama dan terpenting, perlu dicatat bahwa kebijakan penanggulangan Cyber Terrorism melalui hukum pidana termasuk penal policy, yang merupakan bagian dari criminal policy (kebijakan penanggulangan kejahatan). Dari sudut pandang kebijakan pidana, penanggulangan tindak pidana Cyberterrorism memerlukan pendekatan sistematis dan integral. Cyberterrorism adalah salah satu jenis kejahatan tinggi teknologi (high tech crime)[15] yang dapat melintasi batas negara (transnasional/lintas negara). Oleh karena itu, wajar jika penanggulangan Cyber Terrorism juga menggunakan pendekatan teknologi. Selain itu, pendekatan budaya/kultural, moral/pendidikan, dan bahkan global—kerja sama internasional—semuanya diperlukan.[16]

Kebanyakan rumusan tindak pidana di KUHP masih bersifat konvensional dan tidak secara langsung terkait dengan perkembangan cyber terroris, yang merupakan bagian dari cyber crime. Selain itu, ia memiliki berbagai kelemahan dan keterbatasan dalam menangani berbagai perkembangan teknologi dan tindak pidana tinggi yang sangat beragam. Karena tidak ada ketentuan khusus yang mengatur perbuatan kartu kredit palsu, KUHP mengalami kesulitan untuk menangani hanya masalah transfer dana elektronik dan pemalsuan kartu kredit.

Dalam hal ini, untuk menentukan apakah KUHP dapat digunakan untuk menangani tindak pidana cyber terrorism, yang merupakan bagian dari cyber crime, penulis berikut diidentifikasi: kejahatan terhadap ketertiban umum Bab V Pasal 168 ayat 1,2, dan 3; kejahatan terhadap nyawa Bab XIX Pasal 340; pencurian Bab XXII Pasal 362; pemerasan dan pengancaman Bab XXIII Pasal 368.

---

[14] Soerjono Soekanto Dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Ed. 1, Cet, 5, (Jakarta: Raja Grafindo Persada, 2001), hlm. 251-252.

[15] Barda Nawawi Arief, 2002, Tindak Pidana Mayantara, Perkembangan Kajian Cyber Crime Di Indonesia, (Jakarta: PT. Raja Grafindo Persada, 2003), hlm. 90.

[16] Barda Nawawi Arief, Sari Kuliah Perbandingan Hukum Pidana (Jakarta: PT Raja Grafindo, 2002) hlm 253-256

Jika KUHP digunakan untuk menangani tindak pidana cyber terrorism, seseorang harus mempertimbangkan terlebih dahulu batasan, ruang lingkup, dan elemen-elemen cyber terrorism yang telah dijelaskan oleh penulis sebelum mengklasifikasikan tindak pidana cyber terrorism. Komponen termasuk:

1. Serangannya melalui dunia maya bermotivasi politik yang dapat mengakibatkan kematian atau cedera fisik.
2. Menimbulkan ketakutan atau merugikan secara fisik terhadap tekhik serangan dunia maya.
3. Serangannya serius untuk melawan atau ditujukan ke infrastruktur informasi kritis seperti keuangan, energi, transportasi, dan operasi pemerintah.
4. Serangan yang mengganggu sarana yang tidak penting tidak dikategorikan sebagai cyber terrorism.
5. Serangan tidak hanya berfokus pada keuntungan finansial.

Oleh karena itu, berdasarkan penjelasan di atas tentang komponen dan jenis tindak pidana cyber terrorism, penulis berpendapat bahwa Kitab Undang-undang Hukum Pidana tidak dapat digunakan untuk menangani tindak pidana cyber terrorism.

Saat ini, ada undang-undang di luar KUHP yang berkaitan dengan kejahatan yang berkaitan dengan teknologi canggih di bidang informasi, elektronik, dan telekomunikasi, yaitu sebagai berikut:

1. Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektonik Indonesia telah mengesahkan salah satu Rancangan Undang-undang yang berkaitan dengan kejahatan dunia maya (cyber crime), yaitu Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektonik (juga dikenal sebagai UU ITE
2. UU No. 36 Tahun 1999 tentang Telekomunikasi
   Peraturan ini dikeluarkan dalam Lembaran Negara RI tahun 1999 Nomor 154 pada tanggal 8 September 1999, bersama dengan Peraturan Pemerintah nomor 52 tahun 2000 tentang Peraturan Pemerintah tentang Penyelenggaraan Telekomunikasi Indonesia, yang diterbitkan dalam Lembaran Negara nomor 107 tahun 2000, TLN 3980. Salah satu faktor yang dipertimbangkan saat menyusun Undang-Undang Telekomunikasi adalah bahwa globalisasi dan pertumbuhan teknologi komunikasi yang sangat pesat telah menyebabkan transformasi yang signifikan dalam manajemen dan perspektif tentang telekomunikasi. Dengan mengingat bahwa jaringan internet adalah salah satu

alat atau sarana telekomunikasi yang dapat digunakan untuk menyampaikan dan menerima data, penulis mencoba untuk menyelidiki masalah cyber terrorism ini melalui undang-undang telekomunikasi.

Konferensi PBB ke-6 tahun 1980 di Caracas, Venezuela, mengenai "Crime Trends and crime prevention Strategis" menunjukkan bahwa upaya non-penal memiliki posisi strategis. Cyber terrorism termasuk dalam kategori tindak pidana cyber crime atau perbuatan yang menyalahgunakan teknologi internet, yang dapat menyebabkan ketakutan, kerugian fisik dan psikis, dan serangan terhadap infrastruktur penting suatu negara, mengakibatkan kerugian yang signifikan terhadap target sasarannya. Oleh karena itu, penanggulangan cyber terrorism harus berfokus pada pengaturan penggunaan teknologi internet secara efektif.

Karena pentingnya melindungi cyber terrorism sebagai salah satu jenis cybercrime yang memanfaatkan teknologi internet, ada beberapa langkah yang dapat diambil untuk menjaga sistem informasi berbasis internet, antara lain:[17]

1. Mengontrol akses (control access)
2. Menutup layanan yang tidak digunakan
3. Memasang perlindungan
4. Firewall
5. Pemantau adanya serangan
6. Pemantau integritas sistem
7. Audit: melacak berkas log
8. Back up rutin
9. Penggunaan enkripsi untuk meningkatkan keamanan

B. Upaya Kebijakan Hukum Pidana Yang Akan Datang Untuk Menanggulangi Tindak Pidana Cyber Terrorism di Indonesia

Secara sederhana, upaya penanggulangan kejahatan di jalur penal lebih fokus pada sifat "represif" (penindasan, pemberantasan, atau pemusnahan) sesudah kejahatan terjadi, sedangkan jalur non-penal lebih fokus pada tindakan pencegahan (pencegahan/pengendalian)

[17] Budi Rahadjo, op.cit, hal. 51. Bandingkan dengan pendapat Arianto Mukti Wibowo yang terdapat dalam makalahnya berjudul Keamanan Dalam Teknologi Informasi, makalah pada seminar Nasional RUU Teknologi Informasi, Gradhika Bakti Praja, Semarang, 26 Juli 2001

sebelum kejahatan terjadi. Namun, tindakan represif juga mencakup tindakan pencegahan dalam arti luas.[18]

Berbagai ketentuan pidana Indonesia berasal dari KUHP. KUHP telah diubah tujuh belas kali sejak tahun 1977. Berbeda dengan KUHP WvS yang masih berlaku saat ini, konsep KUHP baru membagi KUHP dalam 2 (dua) buku saja. Dalam Konsep KUHP baru, perluasan asas territorial dan perumusan delik tindak pidana di bidang teknologi informasi dibuat sebagai tanggapan atas kelemahan hukum KUHP dalam menangani masalah cyber terrorism, yang merupakan salah satu jenis cybercrime: Pasal 3 Perundang-undangan Indonesia: "Ketentuan pidana dalam perundang-undangan Indonesia berlaku bagi setiap orang yang di luar wilayah Indonesia melakukan tindak pidana di dalam kendaraan air atau pesawat udara Indonesia."[19]

Seperti yang diketahui, hukum pidana Indonesia (KUHP) tidak mengatur tindak pidana cyber terrorism secara eksplisit. Bab 1 Buku Kedua Bagian Keempat, Paragraf 1 hingga Paragraf 5 dari Konsep KUHP baru membahas tindak pidana terorisme, yang diatur dalam Pasal 242 hingga Pasal 251.

Cyberterrorism termasuk dalam kategori tindak pidana cybercrime atau perbuatan yang menyalahgunakan teknologi internet yang dapat menyebabkan ketakutan, kerugian fisik dan mental, dan serangan terhadap infrastruktur penting suatu negara, mengakibatkan kerugian yang signifikan bagi target sasarannya. Oleh karena itu, penanggulangan cyber terrorism harus berfokus pada pengaturan penggunaan teknologi internet secara sengaja.

Setiap pemerintah memiliki kebijakan yang berbeda-beda, tetapi kebijakan umum biasanya bergantung pada seberapa luas demokrasi dianut di negara tersebut. Beberapa model kebijakan yang dibuat oleh berbagai negara untuk mengatasi maraknya cyber terrorism yang berasal dari penyalahgunaan internet menunjukkan sikap yang sama: kesadaran bahwa teknologi internet bukan hanya membawa perubahan ke arah yang baik tetapi juga berpotensi membawa perubahan ke arah yang buruk.

Kebijakan non-penal atau non-penal policy dapat dibuat dengan meningkatkan peran dan penggunaan teknologi dan alat modern yang berfungsi sebagai penyaring atau filter, biasanya software perlindungan. Kebijakan penanggulangan dapat diterima jika dikombinasikan dengan menyaring perangkat lunaknya. Dari perspektif pendekatan teknologi

---

[18] Sudarto, *Kapita Selekta Hukum pidana*, (Bandung: Alumni, 1986), hlm. 118.

[19] Indonesia, Undang-undang Nomor 1 Tahun 2023 Tentang Kitab Undang-undang Hukum Pidana Pasal 3

(technology prevention)[20], sistem pengaman sistem komputer dan jaringan internet harus ditingkatkan untuk mencegah hacker, cracker, dan cyber terrorism menggunakan internet.

KESIMPULAN

Penelitian ini adalah tahap pertama dalam penegakan kebijakan pidana dan politik pidana di Indonesia, dan fokus penelitian ini adalah aspek kebijakan formulasi dan penal. Kebijakan ini dapat digunakan untuk menangani tindak pidana cyber terrorism. Dengan mempertimbangkan berbagai ketentuan yang telah dikriminalisasikan dalam Undang-undang Pemberantasan Tindak Pidana Terrorisme tersebut, jelas bahwa tindak pidana yang berkaitan dengan penyalahgunaan internet, atau cyber terrorism, akan dikriminalisasikan. pentingnya pengaturan cyber terrorism ini karena ini adalah salah satu jenis cybercrime yang memanfaatkan internet. Oleh karena itu, pengaturan internet harus dilakukan. Dari perspektif teknologi, metode ini dimaksudkan untuk mencegah penyebaran penyalahgunaan internet oleh kaum hacker dan cracker atau cyber terrorism.

Sebagai langkah pertama, KUHP Indonesia yang berlaku saat ini harus diperbarui dan disesuaikan agar kebijakan kriminal yang akan datang menangani tindak pidana cyber terrorism sesuai dengan kondisi masyarakat Indonesia saat ini. Oleh karena itu, KUHP baru harus mempertimbangkan kajian komparatif yang terkait dengan tindak pidana cyber terrorism agar lebih memaksimalkan dalam membangun kebijakan penal dan non-penal yang akan datang. Untuk mencapai peningkatan ini, ada beberapa pendekatan antara lain yang dapat digunakan. Pendekatan Teknologi melibatkan pengaturan akses (control access), penutupan layanan yang tidak digunakan, pemasangan proteksi, firewall, pengawasan adanya serangan, dan pengawasan integritas sistem. Audit mencakup pengawasan berkas log, back-up rutin, dan penggunaan enkripsi untuk meningkatkan keamanan.

Pendekatan Moral/Edukatif dapat dilakukan dengan memberikan pendidikan/pelatihan, khususnya pendidikan kewarganegaraan, dan pelatihan komputer dengan tujuan membantu masyarakat, khususnya dalam hal agama. Hal ini disebabkan oleh fakta bahwa cyberterrorism bukanlah kompetisi atau adu kepintaran dengan menggunakan teknologi informasi dan bukan semat-matai. Pendekatan Budaya Kultural, potensi hasil, seperti pengenalan komputer dan internet kepada masyarakat dan peran masyarakat dalam hal ini.

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

SARAN

Seiring maraknya kejahatan di dunia maya yang semakin canggih, kebijakan kriminalisasi terhadap perbuatan dalam dunia maya harus terus disesuaikan. Hal ini disebabkan oleh tindak pidana yang berkaitan dengan teknologi informasi yang beroperasi secara maya dan tidak mengenal batas negara. Oleh karena itu, pemerintah harus selalu berusaha mengantisipasi bisnis baru yang diatur oleh hukum.
Untuk mengatasi tindak pidana cyber terrorism, kebijakan dan upaya yang sudah ada sebelumnya harus diperbarui secara menyeluruh, termasuk peningkatan menggunakan teknologi.

DAFTAR PUSTAKA

Buku

Arief, Barda Nawawi .*Kapita Selekta Hukum Pidana*, Bandung: Citra Aditya Bhakti, 2003.

_____, *Sari Kuliah Perbandingan Hukum Pidana* (Jakarta: PT Raja Grafindo, 2002) hlm 253-256

_____, *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime, Indonesia*, Jakarta: RajaGrafindo Persada, 2006.

Raharjo, Agus. *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: Citra Aditya Bahkti, 2002.

Ramli, Ahmad M. *Cyber Law dan HAKI Dalam Sistem Hukum di Indonesia*, Bandung: Abacus, 2006.

Soekanto, Soerjono dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Ed. 1, Cet, 5, Jakarta: Raja Grafindo Persada, 2001.

Sholeh, Abdul Rahman. *Pendidikan Agama dan Pengembangn untuk Bangsa*, Jakarta: Raja Grafindo Persada, 2005.

Sudarto. *Kapita Selekta Hukum pidana*, (Bandung: Alumni, 1986), hlm. 118.

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

Wahid, Abdul. *Kejahatan Mayantara*, Bandung: Refika Aditama, 2005.

Wiradipradja, Saefullah. *Penuntun Praktis Metode Penelitian dan Penulisan Karya Ilmiah Hukum,* Cet. 2, Bandung: Keni Media, 2015.

Peraturan Perundang-Undangan

Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

----------. Kitab Undang-Undang Hukum Pidana.

----------. Undang-Undang Republik Indonesia 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, Lembaran Negara Republik Indonesia Tahun 2003 Nomor 45, Tambahan Lembaran Negara Republik Indonesia Nomor 4284.

----------. Undang-Undang Republik Indonesia Undang-Undang 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 Undang-Undang 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 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, Lembaran Negara Republik Indonesia Tahun 2018 Nomor 92, Tambahan Lembaran Negara Republik Indonesia Nomor 6216.

Tesis

Nanda Ivan Natsir, "Kebijakan Kriminal Terhadap Tindak Pidana Cyber Terrorism", Tesis, 2009