CYBER-TERRORISM DARI SUDUT PANDANG HUKUM PIDANA INDONESIA

Jecky Tamora Lumban Tobing
Fakultas Hukum, Universitas Dirgantara Marsekal Suryadarma, Indonesia

Abstract

Cyberterrorism has become a serious threat; it does not only consist of hacking as hackers do, but terrorists have a special interest in the violations committed. Based on Law Number 5 of 2018 concerning Amendments to Law Number 15 of 2003 concerning the Stipulation of Government Regulations in Lieu of Law Number 1 of 2002 concerning the Eradication of Criminal Acts of Terrorism into Law, and how to deal with criminal acts of cyber terrorism in Indonesia. To resolve this problem, normative juridical legal research was carried out using statutory and conceptual regulatory approaches. The research results show that the criminal act of cyberterrorism has not been legally regulated. ITE and the Terrorism Law are the most effective laws for anticipating cyber-terrorism crimes. Because the Criminal Code does not accommodate the crime of cyber terrorism at all, cyber law is intended to provide legal certainty that comprehensively regulates the movement, use and deviation of cybercrimes that use computers as the main tool and benefit from developing technology.
Keywords: Cyberterrorism, Cyber, Terrosism Law

Abstrak

Cyberterrorism telah menjadi ancaman yang serius; itu tidak hanya terdiri dari peretasan seperti yang dilakukan hacker, tetapi teroris memiliki kepentingan khusus dalam pelanggaran yang dilakukan. Berdasarkan Undang-undang 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, dan bagaimana penanggulangan tindak pidana cyber terrorism di Indonesia. Untuk menyelesaikan masalah tersebut, dilakukan penelitian hukum yuridis normatif yang menggunakan pendekatan peraturan perundang-undangan dan konseptual. Hasil penelitian menunjukkan bahwa tindak pidana cyberterrorism belum diatur secara hukum. ITE dan UU Terorisme adalah undang-undang yang paling efektif untuk mengantisipasi tindak pidana cyber-terrorisme. Karena KUHP sama sekali tidak mengakomodasi tindak pidana cyber terrorism, cyber law dimaksudkan untuk memberikan kepastian hukum yang mengatur secara komprehensif pergerakan, penggunaan, dan penyimpangan dari kejahatan cyber yang menggunakan komputer sebagai alat utama dan manfaat dari teknologi yang berkembang.
Kata Kunci: Serangan Siber, Dunia Maya, Tindak Pidana Terorisme

PENDAHULUAN

Cyber terrorism adalah jenis lain dari terorisme dan spionase. Tidak hanya mencakup tindakan peretasan yang melanggar hukum seperti yang dilakukan oleh hacker, tetapi teroris cyber memiliki kepentingan khusus dalam pelanggaran yang dilakukan. Cyber terrorism, menurut Dorothy Denning, adalah serangan-serangan yang melanggar hukum yang melibatkan ancaman terhadap komputer, jaringan, dan informasi yang tersimpan di dalamnya untuk mengintimidasi atau memaksa pemerintahan atau masyarakat di dalamnya untuk tujuan politik atau sosial.[1]

Terorisme dunia maya, juga dikenal sebagai terorisme cyber, adalah jenis kejahatan baru dengan ciri-ciri unik.[2] Cyber terrorism didefinisikan sebagai serangan terhadap infrastruktur nasional yang penting atau intimidasi terhadap warga sipil dan staf pemerintah dengan menggunakan jaringan dan teknologi komputer.[3] Semua negara dapat terkena bahaya cyber terrorism, termasuk Indonesia. Untuk melakukan kegiatan terorisme, penggunaan internet harus diwaspadai karena hampir seluruh fasilitas negara, fasilitas umum, dan kegiatan masyarakat menggunakan jaringan, yang dapat menghubungkan segalanya.

Tindak pidana terorisme masih diketahui sebagai tindak pidana khusus di Indonesia karena pengaturannya yang berada di luar Kitab Undang Undang Hukum Pidana. Undang-undang terbaru tentang tindak pidana terorisme, 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.[4] Pasal 1 Angka 2 mendefinisikan terorisme sebagai "perbuatan yang menggunakan kekerasan atau ancaman kekerasan yang menimbulkan suasana teror atau rasa takut secara meluas, yang dapat menimbulkan korban yang bersifat massal, dan/atau menimbulkan kerusakan atau kehancuran

---

[1] Serge Krasavin, "Computer Crime Research Center (CCRC)", http://www.crime-research.org/library/Cyber:terrorism.htm. Diakses pada anggal 3 September 2023, Pukul 10.59 Wib.

[2] Janet J. Prichard and Laurie E. MacDonald, "Cyber Terorism: A study of the Extent Coverage in Computer Science Textbooks", Journal of Information Technology Education, Vol. 3, 2004, hlm. 279-289

[3] *Ibid*.

[4] 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.

terhadap objek vital yang strategis, iingkungan hidup, fasilitas publik, atau fasilitas internasional dengan motif ideologi, politik, atau gangguan keamanan."[5]

Karena undang-undang ini tidak menjelaskan jenis elektronik yang dimaksud, maka tidak setiap media elektronik yang terhubung ke internet. Penggunaan istilah "bentuk elektronik" harus dikaitkan dengan Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik[6] (sebagai perubahan dari Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik), yang mencakup berbagai bentuk sarana elektronik, seperti informasi elektronik, transaksi elektronik, dan sebagainya, untuk meningkatkan pemahaman tentang terorisme dunia maya.

Saat ini, istilah "cybercrime" mengacu pada tindakan kriminal yang berkaitan dengan dunia maya (juga dikenal sebagai "cyber space") dan yang menggunakan komputer. Beberapa ahli menyamakan cyber crime dengan kejahatan komputer, tetapi ahli lain membedakan keduanya.[7] Pada awalnya, para ahli hukum berkonsentrasi pada perangkat keras (hardware), seperti komputer. Namun, dengan berkembangnya jaringan internet dan teknologi informasi lainnya, perhatian terhadap definisi cybercrime menjadi lebih luas, mencakup semua aktivitas yang dapat dilakukan di dunia maya (cyber space) melalui sistem informasi yang digunakan. Oleh karena itu, kejahatan tersebut didefinisikan sebagai cybercrime bukan hanya karena unsur-unsur hadwarenya, tetapi juga karena mereka dapat berkembang di seluruh dunia yang dikelilingi oleh sistem teknologi informasi yang relevan. Akan lebih masuk akal jika kejahatan cyber didefinisikan sebagai kejahatan teknologi informasi.

Beberapa bentuk kejahatan yang paling sering dikaitkan dengan penggunaan teknologi informasi yang berbasis komputer dan jaringan telekomunikasi adalah sebagai berikut:

1. *Unauthorized Access to Computer Sytem and Service*
   Ini terjadi dengan memasuki sistem jaringan komputer secara tidak sah atau tanpa izin.

---

[5] Indonesia, 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, Pasal 1 angka 2.

[6] 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.

[7] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*, (Jakarta: Rajawali Pers, 2012), hlm. 11.

2. *Illegal Content*
   Ini memasukkan data atau informasi yang tidak benar, tidak etis, atau tidak sah ke internet.

3. *Data Forgery*
   Penipuan data pada dokumen penting yang disimpan dalam sistem komputer.

4. *Cyber Expionage*
   Kegiatan mata-mata terhadap pihak lain dengan memasuki sistem jaringan komputer pihak target.

5. *Cyber Sabotage and Exortion*
   Mengganggu, perusakan, atau penghancuran data, program komputer, atau sistem jaringan komputer yang terhubung ke internet.

6. *Offence Against Intellectual Property*
   Kejahatan ini ditujukan terhadap Hak Atas Kekayaan Intelektual (HAKI) pihak lain di internet, seperti meniru tampilan situs web tertentu.

7. *Infringements of Privacy*
   ini berkaitan dengan data pribadi dan rahasia seseorang. Keterangan pribadi seseorang yang tersimpan secara komputerisasi biasanya menjadi sasaran kejahatan ini.

8. *Cyber Terrorism*
   Cyberterrorism termasuk tindakan yang mengancam pemerintah atau warga negara, termasuk merusak situs pemerintah atau militer.[8]

Hukum Cyber atau Cyberlaw adalah aspek hukum yang mencakup setiap aspek yang berhubungan dengan orang atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet, yang dimulai pada saat online dan memasuki dunia cyber atau maya. Untuk menanggulangi kejahatan teknologi ini, maka sangat diperlukan adanya Cyber Law. Tampaknya tidak ada istilah yang disepakati di Indonesia. Dalam hal ini, istilah-istilah yang dimaksudkan untuk diterjemahkan dari undang-undang cyber, seperti Hukum Sistem Informasi, Hukum Informasi, dan Hukum Telematika (Telekomunikasi dan Informatika).[9]

Tujuan dari penelitian ini adalah untuk mempelajari pengaturan cyber terrorism dari sudut pandang hukum pidana Indonesia, khususnya Undang-undang 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

[8] Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law-Aspek Hukum Teknologi Informas*i, (Bandung: Refika Aditama, 2005), hlm. 26.
[9] Bapenda Jabar, "Pengertian *Cyber Crime* dan *Cyber Law*", https://bapenda.jabarprov.go.id/, diakses pada 26 Februari 2024 pukul 18.29 WIB.

Pidana Terorisme Menjadi Undang-Undang, serta untuk mempelajari dan menganalisis penanggulangan tindak pidana cyber terrorism di Indonesia.

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.[10]

Penelitian hukum doktrinal (doctrinal research) adalah penelitian yang bertujuan untuk memberikan penjelasan yang sistematis mengenai aturan yang mengatur bidang hukum tertentu, menganalisis bagaimana aturan tersebut berhubungan satu sama lain, menjelaskan bagian-bagian dari aturan yang sulit dipahami, dan bahkan mungkin mencakup prediksi bagaimana aturan tertentu akan berkembang di masa mendatang. Penelitian hukum doktrinal adalah jenis penelitian yang berbasis kepustakaan dengan fokus pada analisis sumber hukum primer dan sekunder.[11]

Penulis menggunakan pendekatan perundang-undangan (pandangan undang-undang), pendekatan kasus (pandangan kasus), dan pendekatan konseptual. 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. Penelitian ini menggunakan pendekatan kualitatif, yang berarti menyusunnya secara sistematis dan menghubungkan satu sama lain terkait dengan masalah yang diteliti. Penelitian ini juga mempertimbangkan struktur perundang-undangan dan keyakinan hukum, serta perundang-undangan yang berlaku yang dilaksanakan oleh penegak hukum.[12]

---

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

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

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

HASIL DAN PEMBAHASAN

A. Perspektif Hukum Pidana Indonesia Tentang Cyber Terrorism Berdasarkan Undang-undang Nomor 5 Tahun 2018 Tentang Perubahan Undang-undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme

Salah satu jenis kejahatan siber, termasuk *cyber pornography, cyber harassment*, dan *cyber stalking*, adalah terorisme siber atau *cyberterrorism*.[13] *Cyberterrorism* adalah gabungan terorisme dan dunia maya. [14] Serangan teroris yang menggunakan peralatan jaringan komputer (*cyberspace*) untuk mengganggu sistem infrastruktur negara seperti energi, transportasi, dan operasi pemerintahan atau untuk mengintimidasi pemerintahan atau sekelompok masyarakat sipil dikenal sebagai terorisme siber.[15]

Cyberterrorism belum diatur dalam hukum internasional hingga saat ini. Karena tidak ada undang-undang yang tersedia saat ini, disarankan bahwa ASEAN Convention on Counter Terrorism dan International Convention for the Suppression of Terrorist Bombings dapat digunakan sebagai dasar hukum untuk mempidanakan pelaku cyber terrorism. Indonesia meratifikasi konvensi tersebut melalui Undang-undang Nomor 5 Tahun 2012 tentang Pengesahan ASEAN Convention on Counter Terrorism. Sementara itu, Konvensi Internasional untuk Penghapusan Bom Terrorist telah diratifikasi melalui Undang-undang Nomor 5 Tahun 2006 tentang Pengesahan Konvensi Internasional untuk Penghapusan Bom Terrorist.

KUHP sebagian besar bersifat konvensional dalam perumusan tindak pidananya dan belum secara langsung dikaitkan dengan perkembangan terorisme siber, yang merupakan bagian dari kejahatan siber. Di samping itu, KUHP juga mengandung berbagai kelemahan dan keterbatasan yang terkait dengan berbagai perkembangan teknologi dan kejahatan tinggi. Meskipun demikian, tindak pidana terorisme siber dapat dikenakan pada beberapa pasal Kitab KUHP, seperti kejahatan terhadap ketertiban umum (Bab V), Pasal 168 ayat (1), (2), dan (3),

---

[13] Eka L. Marpaung, Mila Astuti, dan Ali Ibrahim, "Analisis Cyber Law dalam Pemberantasan Cyber Terrorism di Indonesia", Prosiding Annual Research Seminar Computer Science and ICT, Vol. 3, No. 1, 2017, hlm. 18.

[14] Eska N. Sarinastiti dan Nabila K. Vardhani, "Internet dan Terorisme: Menguatnya Aksi Global Cyber Terrorism Melalui New Media", Jurnal Gama Societa, Vol. 1, No. 1, 2018, hlm. 43.

[15] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", dalam https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf, diakses pada 17 Januari 2024 pukul 10.37 WIB.

kejahatan terhadap nyawa (Bab XIX), Pasal 340, pencurian (Bab XXII), Pasal 362, serta pemerasan dan pengancaman (Bab XXIII), Pasal 36.[16]

Berkaitan dengan masalah ini, jika KUHP ingin digunakan untuk menangani tindak pidana terorisme siber, harus diperhatikan terlebih dahulu ruang lingkup, elemen, dan bentuk tindak pidana tersebut sebelum dapat didefinisikan sebagai terorisme siber. Komponen-komponen ini termasuk: [17](i) serangan melalui internet yang bermotivasi politik dan menyebabkan kematian; (ii) menimbulkan ketakutan atau kerusakan fisik sebagai akibat dari serangan dari internet; (iii) serangannya serius untuk melawan atau ditujukan ke infrastruktur informasi penting seperti keuangan, energi, transportasi, dan pemerintahan; (iv) serangan yang mengganggu sarana yang tidak penting tetapi tidak termasuk dalam kategori cyber terrorism.

Selain itu, undang-undang telekomunikasi dapat digunakan untuk menjerat terorisme siber. Berikut ini adalah isi pasal tersebut:

1. Pasal 47 mengandung unsur tindak pidana untuk mengelola jaringan telekomunikasi tanpa izin menteri;
2. Pasal 50 mengandung unsur tindak pidana untuk memperoleh akses ke jaringan telekomunikasi, ke jasa telekomunikasi, dan/atau akses ke jaringan ke telekomunikasi khusus; dan
3. Pasal 52 mengandung unsur tindak pidana untuk memperdagangkan, membuat, merakit, memasukan, dan/atau menggunakan perangkat komunikasi di wilayah yang dilarang oleh menteri.
4. Pasal 53 berisi unsur tindak pidana terkait dengan penggunaan spektrum frekwensi radio dan orbit satelit tanpa ijin pemerintah, tidak sesuai dengan peruntukannya, dan saling menganggu;
5. Pasal 55 berisi unsur tindak pidana terkait dengan penggunaan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi;
6. Pasal 56 berisi unsur tindak pidana terkait dengan penyadapan informasi yang disalurkan melalui jaringan telekomunikasi;
7. Pasal 57 yang mengandung unsur tindak pidana: tidak menjaga kerahasiaan informasi pelanggan yang dikirim dan/atau diterima.

Beberapa pasal Undang-undang ITE, termasuk Pasal 28, 29, 30, 31, 32, 33, 34, 35, 45, dan 52, membatasi tindak pidana cybercrime. Melihat berbagai ketentuan yang telah dikriminalisasi, jelas bahwa penyalahgunaan teknologi infomasi dan transaksi elektronik umumnya dikriminalisasi.[18]

---

[16] Danang Enggartyasto dan Irwan Hafid, "Kebijakan Hukum Pidana Terhadap Upaya Pemberantasan Terorisme Siber di Indonesia", LEXRenaissance No. 1 Vol. 7 JanuariI 2022, hlm. 89.

[17] Zahri bin Yunos, "Addresing Cyber Terrorism Threats" dalam https://observatoire-fic.com/en/addressingcyber-terrorism-threats-by-zahri-bin-yunos-cybe rsecurity-malaisia/, diakses pada 17 Januari 2024 pukul 1057 WIB.

[18] Danang Enggartyasto dan Irwan Hafid, "Kebijakan Hukum Pidana Terhadap Upaya Pemberantasan Terorisme Siber di Indonesia", LEXRenaissance No. 1 Vol. 7 JanuariI 2022, hlm. 90.

Jika Anda melihat Pasal 30 UU ITE, pasal tersebut mengatur penggunaan komputer dan/atau sistem elektronik orang lain dengan cara apa pun yang tidak sah atau melanggar hukum. Perbuatan yang dimaksud dalam pasal tersebut adalah tindakan yang melanggar hukum yang dilakukan oleh seseorang terhadap sistem elektronik milik orang lain dengan tujuan untuk mendapatkan informasi dokumen elektronik, serta upaya penerobosan, pembobolan, dan penjebolan yang melampaui batas sistem keamanan. Selain itu, Pasal 32 dan 33 UU ITE konstruksi mengatur perlindungan informasi dan dokumen elektronik yang dianggap rahasia, baik milik orang lain atau milik publik. Frasa "melawan hukum" muncul di awal paragraf. Tidak jelas apakah yang dimaksudkan dengan kata "hukum" dalam frasa "melawan hukum" dalam doktrin hukum pidana Belanda berdasarkan Memorie van Toelichting atau sejarah pembentukan Kitab Undang-undang Hukum Pidana (KUHP). Jika merujuk pada postulat contra legem facit qui id facit quod lex prohibet; in fraudem vero qui, salvis verbis legis, sententinam ejus circumuenit, maka dapat diartikan bahwa seseorang dinyatakan melawan hukum ketika tindakan yang dilakukan adalah suatu tindakan yang dilarang oleh hukum.[19]

Pada dasarnya, struktur Pasal 30, 32, dan 33 Undang-undang ITE dapat diterapkan dalam proses penegakan hukum untuk mempidana pelaku kejahatan cyber-terrorism. Ketiga pasal membahas bagaimana kejahatan cyber-terrorism bekerja, termasuk mengakses komputer tanpa izin, mengubah, merusak dokumen elektronik yang tersimpan, dan melakukan tindakan apa pun yang dapat mengganggu sistem elektronik. Selain itu, pelaku dapat memasuki sistem jaringan komputer dan mengenskripsikan data sehingga mereka tidak dapat diakses lagi, bahkan jika mereka juga melakukan pemerasan dengan meminta uang.

Namun, pasal tersebut memiliki kekurangan, yaitu lebih mengarah pada tindak pidana terhadap orang. Mengingat bahwa kejahatan cyber-terrorisme memiliki karakteristik serangan yang masif, pasal-pasal Undang-undang ITE tidak memenuhi sifat melawan hukum dalam konteks kejahatan cyber-terrorisme karena ancaman dan serangan melawan hukum hanya dilakukan terhadap komputer, data, dan jaringan yang tersimpan dan bertujuan untuk intimidasi terhadap pemerintah atau masyarakat. Di sini, intimidasi dimaksudkan untuk menimbulkan ketakutan atau teror yang dapat mengancam stabilitas keamanan negara.[20]

[19] Alfendo Yefta Argastya dan Supanto, "Penerapan Hukum Pidana Pada Penyidikan Kepolisian Untuk Menanggulangi Kejahatan Ctber Terrorism", Recidive. Volume 11 Issue 1, 2022, hlm. 18.

[20] Alfendo Yefta Argastya dan Supanto, *Op. Cit*, hlm. 19

Meskipun Undang-undang Terorisme seharusnya mengatur terorisme siber secara menyeluruh, beberapa undang-undang di Indonesia, seperti KUHP, Undang-undang ITE, dan Undang-undang Telekomunikasi, mengatur tindak pidana terorisme siber secara sektoral. Perundang-undangan tentang terorisme siber juga dipengaruhi oleh peraturan yang rinci. Undang-undang ITE lebih sering menjerat organisasi terorisme siber daripada Undang-undang Terorisme sendiri.[21]

B. Penanganan Kriminalitas Cyber Terrorism di Indonesia

Dari perspektif teknologi ini[22], beberapa langkah yang dapat diambil untuk mengamanan sistem informasi berbasis internet adalah sebagai berikut: [23]pengaturan akses (pengendalian akses), penutupan layanan yang tidak digunakan, pemasangan proteksi, firewall, pengawasan adanya serangan, pengawasan integritas sistem, audit: melacak berkas log, dan back up secara otomatis.

Di antara kebijakan yang digunakan dalam penciptaan hukum pidana yang berkaitan dengan tindak pidana cyber terrorism adalah sebagai berikut: Kitab Undang-Undang Hukum Pidana Indonesia (KUHP) mengalami kesulitan dalam menangani masalah pemalsuan kartu kredit dan transfer dana elektronik karena tidak memiliki ketentuan khusus mengenai perbuatan kartu kredit palsu.

Ketentuan yang ada hanya mencakup:

1. Sumpah palsu atau keterangan palsu dalam Bab IX Pasal 242;
2. Pemalsuan mata uang dan uang kertas dalam Bab X Pasal 244-252;
3. Pemalsuan materai dan merek dalam Bab XI Pasal 253-262; dan
4. Pemalsuan surat dalam Bab XII Pasal 263-276.

Dalam hal ini, apakah KUHP dapat digunakan untuk menangani tindak pidana cyber terrorism, yang merupakan bagian dari cybercrime, seperti yang diidentifikasi di bawah ini:

1. Kejahatan terhadap ketertiban umum Bab V Pasal 168 ayat 1,2, dan 3;
2. Kejahatan terhadap nyawa Bab XIX Pasal 340;
3. Pencurian Bab XXII Pasal 362;

---

[21] Danang Enggartyasto dan Irwan Hafid, *Op. Cit*, hlm. 91

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

[23] Agus Rahardjo, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung: Citra Adya, 1996), hlm. 51.

4. Pemerasan dan ancaman Bab XXIII Pasal 368.

Untuk menggunakan KUHP untuk menangani tindak pidana cyber terrorism, perlu diperhatikan batasan, unsur, dan bentuk tindak pidana cyber terrorism sebelum dapat diklasifikasikan sebagai tindak pidana cyber terrorism. Oleh karena itu, berdasarkan penjelasan di atas tentang unsur-unsur dan bentuk tindak pidana cyber terrorism, KUHP tidak dapat digunakan untuk menangani tindak pidana cyber terrorism.

KESIMPULAN

Sebenarnya, belum ada undang-undang yang mengatur tindak pidana cyber-terrorisme. Penulis menguraikan pasal dalam UU Telekomunikasi, UU Pendanaan Terorisme, UU ITE, dan UU Terorisme dalam uraian sebelumnya. Berdasarkan temuan penelitian dan penelitian, penulis berpendapat bahwa UU ITE dan UU Terorisme adalah instrumen hukum yang paling efektif untuk mengantisipasi tindak pidana cyber-terrorisme. Sebagai dasar argumennya, dia berpendapat bahwa KUHP sama sekali tidak menerima tindak pidana yang berkaitan dengan cyber terrorism. Selain itu, jika dilihat dari unsur-unsurnya, jelas bahwa rumusan bentuk tindak pidananya masih bersifat konvensional, sehingga tidak memenuhi kriteria untuk kejahatan cyber terrorism. Selanjutnya, UU Telekomunikasi hanya ditujukan untuk mengatur cara penyelenggara berkomunikasi satu sama lain.

Selain itu, UU Pendanaan Terorisme tidak mengatur tindak pidana cyberterrorism jika dikaitkan dengannya. Dalam UU a quo, hanya mengatur transaksi. Selanjutnya, penulis berpendapat bahwa Pasal 30, Pasal 32, dan Pasal 33 UU ITE memiliki dimensi pengaturan yang dapat mengantisipasi cyber-terrorism. Ini didasarkan pada penafsiran elemen-elemen pasal, yang kemudian dikaitkan dengan cara atau modus operandi tindak pidana cyberterrorism. Selanjutnya dalam UU Terorisme, penulis berpendapat bahwa dari semua pasal yang tercantum dalam UU Terorisme, Pasal 6 paling mirip. itu juga berkaitan dengan istilah ancaman kekerasan yang menimbulkan rasa takut atau teror yang meluas dan menyebabkan korban masal.

Dari sudut pandang kepastian hukum, ketentuan hukum penanggulangan tindak pidana cyber terrorism harus difokuskan pada ketentuan Hukum Dunia maya, juga dikenal sebagai cyber law. Sebagai lex specialis, hukum dunia maya diharapkan dapat memberikan kepastian hukum yang mengatur secara komprehensif pergerakan, penggunaan, dan penyimpangan dari

tindakan kejahatan cyber yang menggunakan komputer sebagai alat. Artinya tidak hanya bergantung pada satu Undang-Undang (umbrella act), meskipun ada Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, atau Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

SARAN

Presiden dan DPR memiliki wewenang untuk membuat kebijakan tentang penanggulangan tindak pidana cyber-terrorisme, seperti merevisi UU ITE atau UU Terorisme dan membuat undang-undang baru untuk mencegah tindak pidana tersebut. karena hukum Indonesia saat ini tidak lengkap mengenai tindak pidana cyber-terrorism. Politik hukum pidana dapat digunakan untuk membuat kebijakan ini. Mengingat bahwa kejahatan siber akan berkembang pesat seperti modus operandinya, aparat penegak hukum harus meningkatkan profesionalitas dan kemampuan mereka dalam menanganinya.

UCAPAN TERIMA KASIH

Mengucapkan terimakasih kepada:

1. Bapak Marsekal Muda TNI (Purn) Dr. Sungkono, S.E., M.Si., selaku Rektor Universitas Dirgantara Marsekal Suryadarma, Jakarta.
2. Bapak Marsekal Muda TNI (Purn) Dr. Sujono, S.H., M.H., C.Fr.A., selaku Dekan Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma, Jakarta.
3. Bapak Dr. Diding Rahmat, SH., MH., selaku Ketua Program Studi Ilmu Hukum Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma, Jakarta.
4. Bapak Ario Wendra, S.H., M.H., selaku Sekretaris Program Studi Ilmu Hukum Universitas Dirgantara Marsekal Suryadarma, Jakarta.

DAFTAR PUSTAKA

A. BUKU

Arief, Barda Nawawi. *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime, Indonesia*, Jakarta: RajaGrafindo Persada, 2006.

Mansur, Dikdik M. Arief dan Elisatris Gultom, *Cyber Law-Aspek Hukum Teknologi Informas*i, Bandung: Refika Aditama, 2005.

Rahardjo, Agus. *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung: Citra Adya, 1996), hlm. 51.

Suhariyanto, Budi. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*, Jakarta: Rajawali Pers, 2012.

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

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

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

B. PERATURAN PERUNDANG-UNDANGAN

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

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

----------. 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.

----------. 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.

JURNAL

Alfendo Yefta Argastya dan Supanto, "Penerapan Hukum Pidana Pada Penyidikan Kepolisian Untuk Menanggulangi Kejahatan Ctber Terrorism", Recidive. Volume 11 Issue 1, 2022, hlm. 18.

Danang Enggartyasto dan Irwan Hafid, "Kebijakan Hukum Pidana Terhadap Upaya Pemberantasan Terorisme Siber di Indonesia", LEXRenaissance No. 1 Vol. 7 JanuariI 2022, hlm. 90.

Janet J. Prichard and Laurie E. MacDonald, "Cyber Terorism: A study of the Extent Coverage in Computer Science Textbooks", Journal of Information Technology Education, Vol. 3, 2004, hlm. 279-289.

Marpaung, E.L., Mila Astuti, dan Ali Ibrahim, "Analisis Cyber Law dalam Pemberantasan Cyber Terrorism di Indonesia", Prosiding Annual Research Seminar Computer Science and ICT, Vol. 3, No. 1, 2017, hlm. 18.

INTERNET

Bapenda Jabar, "Pengertian *Cyber Crime* dan *Cyber Law*", https://bapenda.jabarprov.go.id/, diakses pada 26 Februari 2024 pukul 18.29 WIB

Serge Krasavin, "Computer Crime Research Center (CCRC)", http://www.crimeresearch.org/library/Cyber:terrorism.htm. Diakses pada anggal 3 September 2023, Pukul 10.59 Wib.