# KEBIJAKAN HUKUM PERTAHANAN SIBER TERINTEGRASI DALAM MENCEGAH *CYBER TERORISM*
# *Integrated Cyber Defense Legal Policy in Preventing Cyber Terrorism*

**Nuril Maghfirah Alifta[1], Bintang Maulana Ishaq[2], Asri Lailatus Sa'adah[3]**
**Fakultas Hukum Universitas Islam Negeri Kiai Haji Achmad Siddiq Jember**
**maghfirahalifta@gmail.com**

**Abstrak:** Di era perkembangan teknologi yang pesat, kita tidak dapat terlepas dari pengaruhnya. Saat ini, hampir setiap orang bergantung pada teknologi dalam kehidupan sehari-hari. Meskipun kemajuan teknologi membawa banyak dampak positif, seperti efisiensi dan kemudahan akses informasi, ada juga dampak negatif yang perlu diperhatikan, salah satunya adalah cyber terrorism. Teknologi, terutama internet, memberikan kemudahan bagi pelaku terorisme untuk menyerang kelompok atau individu tanpa harus bertatap muka, memanfaatkan cyberspace sebagai sarana untuk melakukan aksinya. Baru-baru ini, Indonesia mengalami insiden kebocoran data pada pusat data nasional, yang disebabkan oleh virus Ransomware WannaCry. Kejadian ini menunjukkan bahwa ancaman terorisme tidak hanya terjadi di dunia fisik, tetapi juga dapat meluas ke ranah digital. Situasi ini memicu perhatian terhadap pengaturan dan penanganan kejahatan cyber terrorism di Indonesia. Dalam paper ini, terdapat dua pertanyaan penting yang akan dibahas. Pertama bagaimana problematika pengaturan dalam penanganan kejahatan cyber terrorism terhadap pusat data nasional? Kedua, bagaimana bentuk kebijakan hukum di masa mendatang untuk membangun pertahanan siber terintegrasi guna mencegah cyber terrorism terhadap pusat data nasional? Metode penelitian yang digunakan adalah kualitatif dengan pendekatan konten analisis, bertujuan untuk menjelaskan kebijakan pertahanan siber yang terintegrasi dalam mencegah cyber terrorism. Hasil penelitian ini diharapkan dapat menggambarkan problematika dalam pengaturan penanganan kejahatan cyber terrorism serta memberikan rekomendasi mengenai kebijakan hukum yang perlu diterapkan dalam membangun pertahanan siber yang lebih efektif untuk melindungi pusat data nasional dari ancaman di dunia maya.
**Kata Kunci:** cyber terrorism; teknologi; pusat data nasional

***Abstract:*** *In the era of rapid development of technology, we cannot let go of its influence when almost everyone depends on technology in life every day. Even though progressive technology brings Lots of positives, such as efficiency And the convenience of accessing information, there is also a impact negative that needs to be noted, wrong the only one is cyber terrorism. Technology, especially the internet, provides convenience for perpetrators of terrorism For attack groups or individuals without face-to-face face, take advantage of cyberspace as a means For doing his actions. Recently, Indonesia has been experiencing incident data leak in the national data center, which is caused by Ransomware virus WannaCry. Incident This shows that threat terrorism is not only happening in the world physical, but Also can expand to digital realm. Situation This triggered attention to the arrangement And Handling of crime cyber terrorism in Indonesia. In this paper, there are two questions important that will be discussed. First How problematic is the arrangement in Handling crime cyber terrorism to the national data center? Second, how to form policy laws in the future To build defense cyber integrated use to prevent cyber terrorism to*

*the national data center? Method research used is qualitative with approach content analysis, aims To explain policy defense integrated cyber in preventing cyber terrorism. Results study This expectation can describe problems in the arrangement of Handling crime cyber terrorism as well as give recommendations about policy and the necessary law applied in building defense more cyber effective To protect national data centers from threats in the world virtual.*
***Keywords:*** *cyber terrorism; technology; national data center*

## PENDAHULUAN

Manusia adalah makhluk sosial yang saling membutuhkan antara satu dengan yang lain. Itu artinya manusia saling membutuhkan informasi atau dengan kata lain saling berhubungan antar manusia lain. Integrasi suatu hubungan sosial memiliki kekuatan sosial juga yang menimbulkan efek lebih besar. Di setiap pekerjaan dan di segala kondisi kita pasti membutuhkan orang lain untuk saling bersinergi, karena tidak semua orang ahli dalam semua bidang. Di usia kemerdekaannya yang sudah menginjak 79 tahun kemerdekaan, Negara Kesatuan Republik Indonesia (NKRI) telah mengalami beberapa transformasi baik dari segi kebudayaan, pendidikan, sosial, budaya, hukum, dan lain-lain. Pada era kolonialisme penggunaan alat tidaklah secanggih zaman sekarang, maka tidak heran jika Indonesia hingga sekarang terus berbenah diri menjadi bangsa yang mandiri dan maju. Transformasi di era digital ini sangat diperlukan, karena perkembangan zaman dan teknologi per tahun-nya terus meningkat.

Dewasa ini dicirikan dengan fenomena kemajuan teknologi informasi dan komunikasi dalam berbagai aspek kehidupan manusia. Perkembangan teknologi informasi dan komunikasi menyebabkan adanya media baru berupa internet yang menyebabkan hubungan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan.[1] Kehidupan manusia di zaman sekarang ini sangat bergantung pada teknologi. Di satu sisi, teknologi dapat membawa banyak dampak positif, seperti adanya *email*, *e-commerce, cyber bank, online business, internet banking*, dan sebagainya. Namun, di sisi lain juga membawa dampak negatif dengan munculnya *cyber terorism*. Kemajuan teknologi membawa tuntutan tersendiri dalam kehidupan masyarakat dalam ketentuan kebutuhan masyarakat, pemerintah dan regulasi yang mengatur kehidupan dalam ruang terbuka atas penggunaan teknologi informasi yang berkembang dan membawa dampak perubahan perilaku budaya hukum dengan sebuah pertanggungjawaban dalam pola hukum baru.[2]

[1] April Laksana, "Pelanggaran Digital Sebagai Tindak Kejahatan dalam Hukum Pidana pada Undang-Undang ITE," *Jurnal Pendidikan Tambusai* 8, no. 2 (2024): 18346–53.
[2] Sri Ayu Astuti, "Law Enforcement of Cyber Terorism in Indonesia," *Rechtsidee* 2, no. 2 (1 Desember 2015): 157–78, https://doi.org/10.21070/jihr.v2i2.82.

*Cyber terrorism* merupakan penggunaan peralatan jaringan komputer untuk mengganggu sistem infrastruktur Negara (energi, transportasi, operasional pemerintahan, dan sejenisnya) atau untuk mengintimidasi pemerintahan atau sekelompok masyarakat sipil. *Cyberspace* dapat digunakan untuk mengalahkan sistem dan menghindari inspeksi.[3] Teroris di beberapa Negara dapat bertukar *email* dengan sedikit ketakutan akan diawasi. Teroris bisa bertemu secara *online* dan menghindari pengecekan imigrasi dengan menggunakan *cyberspace*. Jadi, *cyberspace* menawarkan para teroris keamanan yang lebih kuat dan fleksibilitas operasional. Mereka dapat meluncurkan serangan dari hampir semua tempat di dunia tanpa secara langsung mengekspos diri mereka yang membahayakan diri mereka secara fisik.[4]

Maraknya kasus terorisme siber secara global maupun spesifik di Indonesia, membuat persoalan terorisme semakin kompleks. Salah satu kasus terorisme siber yang pernah menghebohkan publik ialah munculnya serangan virus *ransomware wannacry* terhadap beberapa rumah sakit di hampir 100 negara di seluruh dunia, termasuk Indonesia.[5] Munculnya virus tersebut diduga akibat serangan yang menggunakan media internet untuk membuat sistem komputer dan peralatan teknologi rumah sakit lumpuh. Akibatnya pelayanan rumah sakit menjadi berantakan, seperti sulitnya pasien dan dokter mengakses rekam medis karena gangguan komputer. Pengaturan terorisme siber di Indonesia saat ini bersifat sektoral, baik dalam Kitab Undang-Undang Hukum Pidana (KUHP), UU No. 11 Tahun 2008. tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan UU No. 19 Tahun 2016 (UU ITE), UU No. 36 Tahun 1999 tentang Telekomunikasi, dan UU No. 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang sebagaimana telah diubah dengan UU No. 5 Tahun 2018 (UU Terorisme). Pengaturan *a quo* lebih bersifat gangguan terhadap ketertiban umum yang dilakukan oleh setiap orang dengan perantara telekomunikasi dan teknologi sehingga tidak terlalu menjangkau aturan secara spesifik tindakan teroris yang memanfaatkan teknologi dalam aksinya.

Terorisme siber atau *cyber terrorism* ini merupakan kejahatan jenis baru. Pelaku dalam kejahatan ini dapat perorangan maupun berkelompok/korporasi/badan hukum. Rumusan delik dalam konstruksi pasal undang-undang tentunya harus dapat

[3] Ardison Asri, Lasmauli Noverita Simarmata, dan Aria Caesar Kusuma Atmaja, "Anti Terorisme Siber: Upaya Antisipatif Penanggulangan Terorisme Siber di Indonesia," *Jurnal Ilmiah Hukum Dirgantara* 15, no. 1 (2024): 1–13.
[4] Eska Nia Sarinastiti, "Internet dan Terorisme: Menguatnya Aksi Global Cyber-Terrorism Melalui New Media," *Jurnal Gama Societa* 1, no. 1 (2018): 40–52.
[5] Danang Enggartyasto, "Kebijakan Hukum Pidana Terhadap Upaya Pemberantasan Terorisme Siber di Indonesia," *Lex Renaissance* 7, no. 1 (2022): 84–99.

mengakomodir kejahatan tersebut agar dapat dipertanggungjawabkan secara pidana. Sesuai asas legalitas dalam hukum pidana yaitu "*nullum delictum nulla poena sine praevia lege*" yang berarti bahwa suatu perbuatan tidak dapat dipidana apabila sebelumnya tidak diatur dalam peraturan hukum. Sehingga hal tersebut menciptakan kepastian hukum. Sebab kekosongan hukum berakibat pada terhapusnya pertanggungjawaban suatu kejahatan.[6] Dalam melakukan penyelesaian suatu rumusan masalah terkait *cyber terorism* ini, dibutuhkan integrasi antara 1 instansi dengan instansi yang lain guna saling bersinegritas mewujudkan kepentingan nasional dan keamanan nasional melalui ruang *cyber*.

## METODE PENELITIAN

Metode penelitian yang digunakan adalah menggunakan metode yuridis normatif dengan studi literatur. Studi literatur meneliti data sekunder berupa bahan hukum primer dan bahan hukum sekunder. Dalam penelitian ini menganalisis Peraturan Perundang-Undangan yang berkaitan dengan tindak pidana penyebaran pornografi, yaitu KUHP, UU Tindak Pidana Terorisme dan UU ITE serta RUU KUHP yang dimasa mendatang akan menjadi Peraturan Perundang- Undangan di Indonesia. Selain itu, dalam penelitian ini juga melakukan kajian perbandingan dengan negara-negara lain terkait dengan pengaturan tindak pidana *cyber terorism*. Metode yang digunakan untuk menganalisis data yang terkumpul dalam penelitian ini adalah metode analisis kualitatif.[7] Penelitian yuridis normatif yang bersifat kualitatif adalah penelitian yang mengacu pada norma hukum yang terdapat dalam peraturan perundang-undangan dan putusan pengadilan serta norma-norma yang hidup dan berkembang dalam masyarakat.

## ANALISIS DAN DISKUSI 1

### 1. Problematika Pengaturan dalam Penanganan Kejahatan Cyber Terrorism Terhadap Pusat Data Nasional

*Cyber terrorism* mengacu pada tindakan kriminal yang mengeksploitasi kemajuan teknologi untuk menimbulkan bahaya atau menanamkan ketakutan, seringkali menargetkan infrastruktur pemerintah atau sipil. Hal ini muncul dari penyalahgunaan *system computer* dan internet, dimotivasi oleh kepentingan

[6] Gefbi Nopitasari dan Riska Andi Fitriono, "Pertanggungjawaban Pidana Pelaku Kejahatan Cyber Terrorism Dalam Undang-Undang Nasional," *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi* 1, no. 4 (2024): 180–99.
[7] Burhan Bungin, *Metodologi Penelitian Kualitatif: Aktualisasi Metodologis Ke Arah Ragam Varian Kontemporer* (Jakarta: Penerbit Universitas Indonesia, 2007).

kelompok tertentu untuk menegaskan kehadiran mereka di panggung politik global.[8] Secara umum, *cyber terrorism* dapat didefinisikan sebagai serangkaian aksi ilegal yang direncanakan dan dilakukan oleh individu atau kelompok tertentu. Tindakan ini umumnya dilatarbelakangi oleh motif politik dan bertujuan untuk mewujudkan ideologi mereka. Para pelaku terorisme siber melancarkan serangan baik secara langsung maupun tidak langsung, dengan cara-cara seperti penyusupan, pencurian, atau perusakan terhadap data informasi, sistem komputer, dan program komputer. Akibat dari tindakan ini dapat menimbulkan korban dan kerugian yang signifikan. Selain itu, *cyber terrorism* juga ditandai dengan tindakan yang mengganggu infrastruktur penting, mengintimidasi pemerintahan, dan menyebarkan ideologi melalui sarana digital. Hal ini mencakup berbagai kegiatan, termasuk peretasan, pelanggaran data, dan penyebaran propaganda, sering dilakukan dengan presisi dan anonimitas tinggi.[9]

Fenomena *cyber terrorism* dapat dibagi menjadi dua kategori utama berdasarkan karakteristiknya. Pertama, *cyber terrorism* dipahami sebagai serangan yang ditujukan langsung pada infrastruktur digital. Ini mencakup tindakan-tindakan yang menargetkan sistem komputasi, jaringan komunikasi, serta repositori data dan informasi yang tersimpan dalam perangkat digital. Kategori kedua memandang *cyber terrorism* dari sudut pemanfaatan teknologi internet oleh kelompok-kelompok teroris.[10] Dalam konteks ini, internet digunakan sebagai sarana untuk mengelola aktivitas organisasi teroris dan sebagai platform untuk menyebarkan teror, baik terhadap institusi pemerintah maupun masyarakat umum. Kedua bentuk ini menggambarkan kompleksitas ancaman *cyber terrorism*, yang tidak hanya berfokus pada perusakan infrastruktur digital, tetapi juga memanfaatkan teknologi informasi sebagai alat untuk memperluas jangkauan dan dampak aktivitas terorisme.

Pengaturan terorisme siber di Indonesia saat ini bersifat sektoral, baik dalam Kitab Undang-Undang Hukum Pidana (KUHP), UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan UU No. 19 Tahun 2016 (UU ITE), UU No. 36 Tahun 1999 tentang Telekomunikasi, dan UU No. 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang sebagaimana telah diubah dengan UU No. 5 Tahun 2018 (UU Terorisme). Sehingga ketika terjadi *cyber terrorism* terhadap pusat data nasional maka yang harus menyelesaikan adalah instansi masing masing, hal ini yang menjadi kelemahan dari pemerintah Indonesia dalam menangani kasus *cyber terrorism*.

---

[8] Putu Sekarwangi Saraswati dan I Nengah Susrama, "Pengaturan Cyber Terrorism Ditinjau dari Perspektif Organizational Transnational Crime," *JPPI (Jurnal Penelitian Pendidikan Indonesia)* 10, no. 2 (20 Juni 2024): 308–16, https://doi.org/10.29210/020243153.

[9] Weldi Rozika, "Propaganda dan Penyebaran Ideologi Terorisme Melalui Media Internet (Studi Kasus Pelaku Cyber Terorisme oleh Bahrun Naim)," *Jurnal Ilmu Kepolisian* 11, no. 2 (10 April 2019): 122–34, https://doi.org/10.35879/jik.v11i2.89.

[10] Alfendo Yefta Argastya dan Supanto, "Penerapan Hukum Pidana Pada Penyidikan Kepolisian Untuk Menanggulangi Kejahatan Cyber-Terrorism," *Recidive : Jurnal Hukum Pidana dan Penanggulangan Kejahatan* 11, no. 1 (18 November 2022): 10–28, https://doi.org/10.20961/recidive.v11i1.67425.

## ANALISIS DAN DISKUSI 2

### 1. Sistem Terintegrasi dalam Pencegahan *Cyber*

Keamanan siber dan pertahanan siber mempunyai kaitan yang cukup erat, yaitu keduanya digunakan untuk melindungi dan menjaga kerahasiaan, integritas, dan ketersediaan data elektronik atau sistem elektronik, keamanan siber dapat menjadi salah satu bentuk dari pertahanan siber.[11] Di lain pihak, pertahanan siber dapat menjadi pertahanan aktif maupun pertahanan pasif. Pertahanan pasif yang relevan dapat dimasukkan dalam bidang keamanan siber. Data dan informasi merupakan sumber daya yang penting untuk suatu badan atau lembaga di era digital saat ini. Ketersediaan, kemudahan penggunaan, dan keamanan informasi harus diperhatikan agar informasi tetap tersedia untuk publik. Salah satu hal yang dapat mengganggu ketersediaan data yaitu ancaman siber. Untuk melindungi data dan menghindari segala ancaman siber, keamanan siber (*cyber security*) harus diterapkan. Keamanan siber (*cybersecurity*) adalah upaya untuk menjaga kerahasiaan, keutuhan dan ketersediaan informasi dari serangan digital. Keamanan siber mengacu pada keamanan informasi digital yang disimpan di jaringan elektronik, serta keamanan jaringan yang menyimpan dan mengirimkan informasi.[12]

Namun, ada sedikit pengertian tentang bagaimana sebenarnya itu didefinisikan. Keamanan siber kadang-kadang digunakan bergantian dengan keamanan informasi. Keamanan informasi dan siber pada umumnya merujuk untuk hal yang sama. Namun, keamanan informasi digunakan oleh organisasi dan TI profesional, sementara keamanan siber lebih umum digunakan dalam kebijakan, dan ketika masalah keamanan informasi terbentuk sebagai masalah keamanan nasional. Keamanan siber memiliki peran yang sangat penting, maka dari itu, negara hadir melalui Badan Siber dan Sandi Negara (BSSN) dengan membentuk *Computer Security Incident Response Team* (CSIRT) sebagai salah satu eksekutor keamanan siber di Indonesia. *Computer Security Incident Response Team* (CSIRT) adalah tim yang menyediakan layanan untuk mencegah, mengatasi dan menanggapi insiden keamanan siber di suatu wilayah yang

[11] Muhammad Prakoso Aji, "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)," *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 13, no. 2 (4 Januari 2023): 222–38, https://doi.org/10.22212/jp.v13i2.3299.

[12] Moh Riskiyadi, Alexander Anggono, dan Tarjo, "Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis," *Jurnal Manajemen dan Organisasi* 12, no. 3 (29 Desember 2021): 239–51, https://doi.org/10.29244/jmo.v12i3.33528.

bertanggung jawab, untuk penerimaan, peninjauan dan penindakan laporan dan aksi insiden keamanan siber.[13]

Penegakan hukum terkait *cyber terrorism* tidaklah mudah, mengingat karakteristik dari kejahatan tersebut. Beberapa yang menjadi kendala Penanganan *cyber terrorism* antara lain:

a. Tidak ada definisi hukum yang secara pasti mengenai apa itu kejahatan *cyber terrorism* meskipun telah terdapat beberapa pendapat dari para ahli.
b. Formulasi hukum di Indonesia belum dapat menjangkau terkait perkembangan kejahatan pada dunia maya terutama pada *cyber terrorism*, bahkan undang-undang yang terkait mengenai perlindungan data pribadi belum ada di Indonesia, dan untuk sementara ini pengaturan tentang kejahatan dunia maya didasarkan pada Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-undang Nomor 11 Tahun 2008.
c. Keunikan pada kejahatan dunia maya adalah kejahatan tersebut dapat melintasi sebuah yuridiksi negara, sementara itu masih sedikitnya perjanjian internasional yang mengatur mengenai penegakan hukum *cyber terrorism*.
d. Perlu adanya keseimbangan antara tindakan represif maupun preventif dalam mengatasi masalah *cyber terrorism*.
e. Kurangnya kewaspadaan para pengguna internet di tanah air yang memungkinkan menjadi suatu korban kejahatan siber, seperti memberikan identitas pribadi, foto, maupun video kepada orang yang baru saja dikenal.

Pembentukan undang-undang yang mengatur secara khusus tentang *cyber crime* merupakan hal yang sangat penting terlebih kejahatan tersebut merupakan *extra ordinary crime* yang dimana memerlukan penanganan khusus. Terdapat 4 alternatif guna menangani *cyber crime* yaitu:[14]

a. Memperluas pengertian maupun istilah tertentu melalui penafsiran hukum pada KUHP konvensional.
b. Melakukan amandemen KUHP.
c. Menerbitkan peraturan secara khusus yang mengatur *cyber crime* yang didalamnya juga terdapat delik mengenai *cyber terrorism*.

[13] Dewi Rizka Yuniarti dkk., "Analisis Potensi dan Strategi Pencegahan Cyber Crime dalam Sistem Logistik di Era Digital," *Jurnal Bisnis, Logistik dan Supply Chain (BLOGCHAIN)* 3, no. 1 (23 Juni 2023): 23–32, https://doi.org/10.55122/blogchain.v3i1.714.
[14] Duarif dan Moh. Saleh, "Pencegahan dan Penindakan Tindak Pidana Siber oleh Kepolisian Resort Teluk Bintuni," *UNES Law Review* 6, no. 4 (2024): 12110–19.

d. Mengamandemen KUHP sekaligus menerbitkan Undang-Undang khusus yang mengatur *cyber crime*.

Munculnya beragam jenis kejahatan siber termasuk *cyber terrorism* dapat disebabkan oleh beberapa faktor keamanan, selain itu kurangnya wawasan para penegak hukum dalam menindak para pelaku kejahatan siber, serta belum adanya undang-undang yang mengatur secara khusus mengenai *cyber crime* dan dapat memberikan celah bagi para pelaku tindak pidana *cyber terrorism*. Kongres PBB VIII/1990 mengenai "*computer-related crimes*" dalam upaya menanggulangi kejahatan *cyber terrorsim* mengajukan beberapa kebijakan antara lain:[15]

a. Menghimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:
   - Melakukan modernisasi hukum pidana.
   - Mengembangkan tindakan-tindakan pencegahan keamanan komputer.
   - Melakukan sosialisasi hukum kepada masyarakat mengenai *cyber terrorism* serta memberikan wawasan bagi para penegak hukum terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer.
   - Melakukan training bagi para hakim, pejabat dan aparat penegak hukum mengenai *cyber crime*.
b. Menghimbau negara anggota meningkatkan kegiatan nasional dalam upaya penangggulangan *cyber terrrosim* yang juga sebagai bentuk kejahatan siber. Berkaitan dengan resolusi kongres PBB VIII/1990 terkait *computer-related crime*, bahwa dalam upaya penanggulangan *cyber terrorism* Indonesia dituntut untuk melakukan modernisasi hukum pidana. Dalam seminarnya Wigrantoro Roes Setiyadi mengenai *cyber crime* tanggal 19 Maret 2003 beliau menawarkan alternatif diantaranya adalah:
   - Menghapus pasal-pasal dalam UU terkait yang tidak dipakai lagi.
   - Mengamandemen KUHP.
   - Mensisipkan hasil kajian dalam RUU yang ada.
   - Membuat RUU khusus *cyber crime*.

Adapun pola integrasi siber sebagai bentuk pencegahan yang dapat dilakukan pemerintah dimasa mendatang yaitu:

a. Kolaborasi dengan lembaga-lembaga terkait.

[15] Ilham Ghani Indrayanto, Eko Soponyono, dan Mujiono Hafidh Prasetyo, "Kebijakan Penal Penanggulangan Cyber Terrorism di Masa Sekarang Maupun di Masa Mendatang," *Diponegoro Law Journal* 11, no. 4 (2022): 1–15.

Kolaborasi lembaga merupakan suatu kerjasama berbagai lembaga Negara yang ada di pusat dan daerah seperti Kemenkominfo pusat di Jakarta, kominfo daerah baik kota maupun kabupaten di 10 kabupaten kota yang ada di NTB yang berperan memberikan keterangan ahli maupun data otentik baik pelaku maupun korban. PT. Telkom Indonesia tbk di daerah NTB yang bertugas memberikan penjelasan ahli tentang manfaat alat telekomunikasi sebagai sarana menyampaikan informasi secara cepat, mudah dan praktis melalui keterangan ahli. Kantor Pengadilan Negeri berperan membantu kami dalam penyelesaian kasus apabila kasus tersebut sudah masuk SP2HP untuk dilakukan dalam penyelidikan, pemutusan, dan pemberian sanksi pidana atau dibebaskan.

b. Melakukan Patroli Siber
   Patroli siber merupakan kegiatan yang dilakukan rajia online melalui system program Aplikasi Patroli Siber Polri untuk mengamati, mengawasi perkembangan media social baik facebook, twitter, email, whatshap, line, dan instagram, maupun penggunaan internet lainnya dalam waktu berkala yaitu dalam waktu 3 hari sekali, mingguan, bulanan dan tahunan. Aplikasi Patroli Siber Polri ini berkerja selama 24 jam/hari dengan tujuan mengidentifikasi berita hoax, penipuan online, pencemaran nama baik, pelecehan seksual, ujaran kebencian, ujaran kebencian yang dilakukan masyarakat baik akun pribadi maupun akun kelompok.
c. Upaya Pencegahan melalui Penyuluhan, Edukasi, Kampanye dan Pendampingan (PEKP) Upaya pencegahan melalui penyuluhan, edukasi, kampanye dan pendampingan (PEKP) kepada masyarakat baik melalui media cetak, *online* maupun secara pendampingan. Penyuluhan dilakukan di instansi sekolah, desa dan tempat-tempat umum dengan melibatkan OKP.
d. Menjaga identitas
   Dalam sistem integrasi siber tersebut, ada beberapa yang kami lakukan yaitu bekerjasama dengan mitra lembaga Negara seperti Polda dengan Dinas Kominfo terdekat, Polda dengan PT. Telkom, Polda dengan Pengadilan negeri setempat ketiga lembaga tersebut cukup bagus dalam membantu menyelesaikan berbagai kasus kejahatan.[16]

Adapun Dasar hukum penggunaan teknologi dan informatika elektronik tercantum dalam Undang-Undang Nomor 11 Tahun 2008 pada Pasal 1: Ayat (1) "*Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi*

[16] Abdul Sakban dan Zaini Bidaya, "Desain Pola Integrasi Cyber dalam Mengurangi Kejahatan Cyberbullying," *CIVICUS: Pendidikan, Penelitian, Pengabdian Pendidikan Pancasila dan Kewarganegaraan* 9, no. 1 (2021): 38–46.

*tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya*."

## PENUTUP

Berdasarkan hasil pembahasan di atas bahwasanya di Indonesia belum terdapat peraturan yang secara eksplisit mengatur tindak pidana *cyber terrorism* baik dalam UU ITE maupun UU Terorisme, oleh karenanya masih dalam hal menindak para pelaku kejahatan siber masih belum maksimal dan masih terdapat penggunaan-penggunaan pasal yang tidak semestinya seperti penerapan pasal dalam KUHP yang dikenakan pada pelaku tindak kejahatan siber. Berdasarkan hasil penelitian di atas, kebijakan penal penanggulangan di masa mendatang telah dirumuskan dalam beberapa rancangan undang-undang terkait *cyber crime* dan telah diatur juga pada RUU KUHP. Oleh karenanya pengesahan RUU KUHP sangatlah penting karena dalam pembentukan Rancangan Undang-Undang terkait *cyber terrorism* diperlukan RUU KUHP sebagai payung hukum daripada *cyber law*.

## DAFTAR PUSTAKA

Abdul Sakban dan Zaini Bidaya. "Desain Pola Integrasi Cyber dalam Mengurangi Kejahatan Cyberbullying." *CIVICUS: Pendidikan, Penelitian, Pengabdian Pendidikan Pancasila dan Kewarganegaraan* 9, no. 1 (2021): 38–46.

Aji, Muhammad Prakoso. "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 13, no. 2 (4 Januari 2023): 222–38. https://doi.org/10.22212/jp.v13i2.3299.

Argastya, Alfendo Yefta dan Supanto. "Penerapan Hukum Pidana Pada Penyidikan Kepolisian Untuk Menanggulangi Kejahatan Cyber-Terrorism." *Recidive : Jurnal Hukum Pidana dan Penanggulangan Kejahatan* 11, no. 1 (18 November 2022): 10–28. https://doi.org/10.20961/recidive.v11i1.67425.

Asri, Ardison, Lasmauli Noverita Simarmata, dan Aria Caesar Kusuma Atmaja. "Anti Terorisme Siber: Upaya Antisipatif Penanggulangan Terorisme Siber di Indonesia." *Jurnal Ilmiah Hukum Dirgantara* 15, no. 1 (2024): 1–13.

Astuti, Sri Ayu. "Law Enforcement of Cyber Terorism in Indonesia." *Rechtsidee* 2, no. 2 (1 Desember 2015): 157–78. https://doi.org/10.21070/jihr.v2i2.82.

Burhan Bungin. *Metodologi Penelitian Kualitatif: Aktualisasi Metodologis Ke Arah Ragam Varian Kontemporer*. Jakarta: Penerbit Universitas Indonesia, 2007.

Danang Enggartyasto. "Kebijakan Hukum Pidana Terhadap Upaya Pemberantasan Terorisme Siber di Indonesia." *Lex Renaissance* 7, no. 1 (2022): 84–99.

Duarif dan Moh. Saleh. "Pencegahan dan Penindakan Tindak Pidana Siber oleh Kepolisian Resort Teluk Bintuni." *UNES Law Review* 6, no. 4 (2024): 12110–19.

Ilham Ghani Indrayanto, Eko Soponyono, dan Mujiono Hafidh Prasetyo. "Kebijakan Penal Penanggulangan Cyber Terrorism di Masa Sekarang Maupun di Masa Mendatang." *Diponegoro Law Journal* 11, no. 4 (2022): 1–15.

Laksana, April. "Pelanggaran Digital Sebagai Tindak Kejahatan dalam Hukum Pidana pada Undang-Undang ITE." *Jurnal Pendidikan Tambusai* 8, no. 2 (2024): 18346–53.

Nopitasari, Gefbi, dan Riska Andi Fitriono. "Pertanggungjawaban Pidana Pelaku Kejahatan Cyber Terrorism Dalam Undang-Undang Nasional." *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi* 1, no. 4 (2024): 180–99.

Riskiyadi, Moh, Alexander Anggono, dan Tarjo. "Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis." *Jurnal Manajemen dan Organisasi* 12, no. 3 (29 Desember 2021): 239–51. https://doi.org/10.29244/jmo.v12i3.33528.

Rozika, Weldi. "Propaganda dan Penyebaran Ideologi Terorisme Melalui Media Internet (Studi Kasus Pelaku Cyber Terorisme oleh Bahrun Naim)." *Jurnal Ilmu Kepolisian* 11, no. 2 (10 April 2019): 122–34. https://doi.org/10.35879/jik.v11i2.89.

Saraswati, Putu Sekarwangi, dan I Nengah Susrama. "Pengaturan Cyber Terrorism Ditinjau dari Perspektif Organizational Transnational Crime." *JPPI (Jurnal Penelitian Pendidikan Indonesia)* 10, no. 2 (20 Juni 2024): 308–16. https://doi.org/10.29210/020243153.

Sarinastiti, Eska Nia. "Internet dan Terorisme: Menguatnya Aksi Global Cyber-Terrorism Melalui New Media." *Jurnal Gama Societa* 1, no. 1 (2018): 40–52.

Yuniarti, Dewi Rizka, Hafidz Fauzan Alfarizy, Zifron Siallagan, dan Mochamad Whilky Rizkyanfi. "Analisis Potensi dan Strategi Pencegahan Cyber Crime dalam Sistem Logistik di Era Digital." *Jurnal Bisnis, Logistik dan Supply Chain (BLOGCHAIN)* 3, no. 1 (23 Juni 2023): 23–32. https://doi.org/10.55122/blogchain.v3i1.714.