Jurnal Hukum Mimbar Justitia (JHMJ)
Vol.: 10, No.2, Desember 2024, h 430-443
ISSN: 2477-5681 (Cetak),
ISSN: 2580-0906 (Online)
Available Online at: jhmj.fh@unsur.ac.id

Evaluasi Efektivitas Undang-Undang No. 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik dalam Pencegahan Cyberterrorism

Evaluation of the Effectiveness of Law No. 1 of 2024 on Information and Electronic Transactions in Preventing Cyberterrorism

Muhammad Arkhan Maulana Bastian[1], Rudy Sutanto[2], Raden Ruli Basuni[3]
[1,2,3] *Universitas Pertahanan*

Article Info

Corresponding Author:
Penulis Korespondensi
✉ *arkandbastian@gmail.com*

History:
Submitted: 10-01-2025
Revised: 14-01-2025
Accepted: 14-01-2025

Kata Kunci:
Cyberterrorism; Evektifitas; alat sarana.

Keyword:
Cyberterrorism; Effectiveness; tools.

https: 10.35194/jhmj.v10i2.4997

Abstrak

Penelitian ini mengevaluasi efektivitas Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) dalam pencegahan terorisme siber di Indonesia. Studi ini menyoroti perlunya kerangka hukum yang kuat untuk mengatasi terorisme siber, yang dapat merusak stabilitas nasional dalam hal politik, ekonomi, dan sosial. UU ITE bertujuan untuk meningkatkan langkah-langkah hukum terhadap kejahatan siber, implementasinya menghadapi tantangan seperti tumpang tindih kewenangan lembaga, infrastruktur teknologi yang terbatas, dan literasi digital publik yang rendah. Menggunakan metode kualitatif, termasuk wawancara dan analisis hukum, penelitian ini mengidentifikasi kekuatan dan kelemahan dalam hukum, menekankan pentingnya mengintegrasikan asuransi siber sebagai strategi pelengkap untuk meningkatkan keamanan digital. Temuan menunjukkan bahwa meningkatkan koordinasi antar-lembaga, meningkatkan kesadaran publik, dan memanfaatkan teknologi pemantauan canggih sangat penting untuk mengoptimalkan efektivitas undang-undang. Pada akhirnya, studi ini memberikan rekomendasi strategis untuk menyempurnakan kebijakan hukum dan mendorong pendekatan kolaboratif antara pemerintah, sektor swasta, dan masyarakat sipil untuk memerangi terorisme siber secara efektif.

Abstract

This research evaluates the effectiveness of Law No. 1 of 2024 on Information and Electronic Transactions (ITE Law) in preventing cyber terrorism in Indonesia. This study highlights the need for a strong legal framework to address cyber terrorism, which can undermine national stability in political, economic, and social aspects. The ITE Law aims to enhance legal measures against cybercrime, but its implementation faces challenges such as overlapping institutional authorities, limited technological infrastructure, and low public digital literacy. Using qualitative methods, including interviews and legal analysis, this research identifies the strengths and weaknesses in the law, emphasizing the importance of integrating cyber insurance as a complementary strategy to enhance digital security. The findings indicate that enhancing inter-agency coordination, increasing public awareness, and leveraging advanced monitoring technology are crucial for optimizing the effectiveness of the law. Ultimately, this study provides strategic recommendations to refine legal policies and encourage a collaborative approach between the government, the private sector, and civil society to effectively combat cyber terrorism.

A. PENDAHULUAN

1. Latar Belakang

Kemajuan teknologi informasi dan komunikasi telah membawa dampak signifikan dalam berbagai aspek kehidupan manusia, termasuk kemudahan akses informasi dan interaksi di dunia maya. Namun, kemajuan ini juga membuka peluang bagi kejahatan berbasis teknologi, salah satunya adalah *cyberterrorism*. *Cyberterrorism* merupakan ancaman serius yang dapat mengganggu stabilitas negara, baik dalam aspek politik, ekonomi, maupun sosial. Kejahatan ini melibatkan penggunaan teknologi informasi untuk melakukan serangan terhadap infrastruktur kritis, penyebaran propaganda radikal, hingga penggalangan dana untuk aktivitas teroris.[1]

Indonesia, sebagai salah satu negara dengan jumlah pengguna internet yang terus meningkat, tidak terlepas dari ancaman *cyberterrorism*. Dalam menghadapi tantangan ini, pemerintah telah mengesahkan Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai revisi dari regulasi sebelumnya. Revisi ini bertujuan untuk memperkuat landasan hukum dalam penanggulangan kejahatan siber, termasuk *cyberterrorism*, dengan mengatur berbagai aspek, seperti penyalahgunaan informasi, perlindungan data, dan penegakan hukum terhadap pelaku kejahatan di dunia maya.[2]

Meskipun demikian, efektivitas UU No. 1 Tahun 2024 dalam mencegah dan menangani kasus *cyberterrorism* masih menjadi pertanyaan. Beberapa pihak menilai bahwa undang-undang ini memiliki sejumlah kelemahan, baik dari sisi substansi hukum, implementasi, maupun koordinasi antarinstansi yang terlibat. Misalnya, masih terdapat interpretasi yang beragam terhadap beberapa pasal dalam UU ITE, serta tantangan dalam menyesuaikan regulasi dengan perkembangan teknologi yang sangat cepat.[3]

Selain itu, tantangan lainnya adalah minimnya kesadaran masyarakat tentang ancaman *cyberterrorism* dan pentingnya literasi digital. Rendahnya pemahaman ini dapat menghambat upaya pencegahan dan deteksi dini terhadap aktivitas mencurigakan di dunia maya. Oleh karena itu, evaluasi terhadap efektivitas UU No. 1 Tahun 2024 menjadi hal yang krusial untuk

---

1 Saptaning Ruju Paminto, "Cyber Terrorism Countermeasures in Indonesia," *Jurnal Wawasan Yuridika* 6, no. 2 (2022): 186–196, https://ejournal.sthb.ac.id/index.php/jwy/article/download/464/226.

2 Saptaning Ruju Paminto et al., "Peran Hukum Dalam Melindungi Korban Penipuan Media Sosial Perspektif Sosiologi," *Journal Customary Law* 2, no. 1 (2024): 1–18, https://journal.pubmedia.id/index.php/jcl/article/view/3335.

3 Rizki Setyobowo Sangalang et al., "Hukum Pidana Cyber: Buku Referensi" (Medan: PT. Media Penerbit Indonesia, 2024).

memastikan bahwa regulasi ini benar-benar mampu memberikan perlindungan yang optimal terhadap ancaman *cyberterrorism*.

Latar belakang ini menjadi dasar bagi penelitian yang bertujuan untuk mengevaluasi sejauh mana efektivitas UU No. 1 Tahun 2024 dalam mencegah *cyberterrorism* di Indonesia. Penelitian ini juga diharapkan dapat memberikan rekomendasi strategis untuk memperbaiki kebijakan hukum di bidang kejahatan siber, serta mendukung upaya pencegahan dan penanggulangan *cyberterrorism* secara menyeluruh.[4]

Sebagai respons terhadap tantangan ini, pemerintah Indonesia telah melakukan pembaruan regulasi melalui Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) yang menggantikan UU No. 19 Tahun 2016. Pembaruan ini dilatarbelakangi oleh kebutuhan akan kerangka hukum yang lebih komprehensif dan adaptif dalam menghadapi evolusi ancaman siber, khususnya *cyberterrorism* yang semakin canggih dan terorganisir.[5]

Beberapa kasus *cyberterrorism* yang terjadi di Indonesia, seperti serangan terhadap infrastruktur digital pemerintah, institusi keuangan, dan fasilitas publik vital, menunjukkan urgensi evaluasi efektivitas regulasi yang ada. Kompleksitas ancaman *cyberterrorism* semakin meningkat dengan penggunaan teknologi mutakhir seperti artificial intelligence, machine learning, dan internet of things (IoT) oleh kelompok teroris dalam melancarkan serangannya.[6]

Keterlibatan Indonesia dalam berbagai kerjasama internasional terkait keamanan siber, seperti *ASEAN Convention on Cybercrime dan International Convention on Cybersecurity*, juga menuntut harmonisasi regulasi nasional dengan standar internasional. Hal ini menjadi pertimbangan penting dalam mengevaluasi efektivitas UU ITE yang baru dalam konteks pencegahan *cyberterrorism*.[7]

Studi tentang efektivitas UU No. 1 Tahun 2024 dalam pencegahan *cyberterrorism* menjadi krusial mengingat dinamika ancaman yang terus berkembang. Evaluasi ini mencakup aspek substansi hukum, struktur penegakan, dan budaya hukum masyarakat dalam

---

4 Fitri Mutia et al., *Bunga Rampai Literasi Dan Perpustakaan Berbasis Inklusi Sosial* (Zifatama Jawara, 2024).

5 Amanda Fitria Najwa and Aqila Husna, "Efektifitas Yurisdiksi Cybercrime Di Tengah Perkembangan Teknologi Informasi," *Jurnal Hukum dan Sosial Politik* 2, no. 3 (2024): 126–135, https://ifrelresearch.org/index.php/jhsp-widyakarya/article/view/3426.

6 Ahmad Budiman et al., *Pembangunan Kekuatan Minimum Komponen Utama Pertahanan Negara Di Era New Normal* (Jakarta: Publica Indonesia Utama, 2021).

7 Fajar B Hirawan, *Indonesia Dan Covid-19: Pandangan Multi Aspek Dan Sektoral* (Jakarta: Centre for Strategic and International Studies, 2020).

mengimplementasikan regulasi tersebut. Analisis mendalam diperlukan untuk mengidentifikasi kesenjangan antara regulasi yang ada dengan tantangan aktual di lapangan, serta merumuskan rekomendasi untuk peningkatan efektivitas pencegahan *cyberterrorism* di Indonesia.[8]

Penelitian ini juga mempertimbangkan aspek keseimbangan antara upaya penegakan hukum dengan perlindungan hak-hak digital warga negara. Evaluasi efektivitas UU ITE dalam pencegahan *cyberterrorism* harus memperhatikan prinsip-prinsip demokrasi, kebebasan berekspresi, dan privasi digital, sambil tetap menjaga kepentingan keamanan nasional.[9]

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengevaluasi sejauh mana UU No. 1 Tahun 2024 tentang ITE efektif dalam mencegah dan menanggulangi ancaman *cyberterrorism* di Indonesia. Hasil penelitian diharapkan dapat memberikan kontribusi signifikan bagi pengembangan kebijakan dan strategi pencegahan *cyberterrorism* yang lebih komprehensif dan adaptif.[10]

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa dampak signifikan terhadap berbagai aspek kehidupan, termasuk munculnya ancaman baru dalam bentuk kejahatan siber, salah satunya adalah *cyberterrorism. Cyberterrorism* merujuk pada penggunaan teknologi informasi untuk melakukan tindakan terorisme yang dapat mengganggu stabilitas sosial, politik, dan ekonomi suatu negara. Di Indonesia, fenomena ini semakin meningkat, sehingga diperlukan regulasi yang efektif untuk menanggulanginya.Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan langkah legislasi terbaru yang bertujuan untuk memberikan kerangka hukum dalam mengatur aktivitas di dunia maya, termasuk pencegahan *cyberterrorism*. UU ini menggantikan Undang-Undang sebelumnya dan memperkenalkan sejumlah perubahan signifikan, termasuk penambahan pasal-pasal baru yang berfokus pada perlindungan masyarakat dari penyalahgunaan teknologi informasi.[11]

Namun, meskipun UU ITE diharapkan dapat memberikan perlindungan yang lebih baik terhadap kejahatan siber, pelaksanaan undang-undang ini masih menghadapi berbagai

---

8 Sangalang et al., "Hukum Pidana Cyber: Buku Referensi."

9 Philemon Ginting, "Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana" (Program Sarjana Universitas Diponegoro, 2008).

10 Sangalang et al., "Hukum Pidana Cyber: Buku Referensi."

11 Masduki Khamdan Muchamad and others, *Kejahatan Siber Ancaman Dan Permasalahannya: Tinjauan Yuridis Pada Upaya Pencegahan Dan Pemberantasannya Di Indonesia* (Banda Aceh: Syiah Kuala University Press, 2023).

tantangan. Penelitian sebelumnya menunjukkan bahwa ada kekurangan dalam kesadaran publik mengenai bahaya cybercrime, lemahnya penegakan hukum, serta perlunya interpretasi yang lebih jelas terhadap pasal-pasal dalam undang-undang tersebut. Selain itu, terdapat kritik mengenai potensi penyalahgunaan kewenangan pemerintah dalam menerapkan undang-undang ini, yang dapat mengancam kebebasan berekspresi masyarakat.[12]

Dengan latar belakang tersebut, evaluasi efektivitas UU No. 1 Tahun 2024 sangat penting dilakukan untuk memahami sejauh mana undang-undang ini mampu mencegah dan menanggulangi *cyberterrorism* di Indonesia. Penelitian ini bertujuan untuk menganalisis implementasi UU ITE dalam konteks pencegahan kejahatan siber serta mengidentifikasi faktor-faktor yang mempengaruhi efektivitasnya. Diharapkan hasil penelitian ini dapat memberikan rekomendasi bagi perbaikan kebijakan hukum dan strategi penegakan hukum di bidang teknologi informasi dan transaksi elektronik.[13]

2. Perumusan Masalah

Penelitian ini perlu mengeksplorasi berbagai aspek seperti celah keamanan dalam infrastruktur digital yang dapat dimanfaatkan oleh pelaku kejahatan yang menyebabkan kesulitan dalam mengidentifikasi dan menindak pelaku kejahatan siber yang sering kali menggunakan metode anonim secara global, dan bagaimana efektivitas Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dalam menanggulangi penyebaran hoaks,

3. Metode Penelitian

Dalam penelitian ini, kami akan menggunakan metode penelitian yang komprehensif dan beragam untuk mengevaluasi efektivitas Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) dalam pencegahan *cyberterrorism*. Metode yang akan digunakan meliputi pendekatan kualitatif, analisis hukum, serta pengumpulan data primer dan sekunder. Pendekatan kualitatif dipilih untuk mendapatkan pemahaman mendalam mengenai pelaksanaan UU ITE dan dampaknya terhadap pencegahan

---

[12] Adinda Lola Sariani Dinda, "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia," *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum* 2, no. 2 (2024): 69–77, https://ejournal.indrainstitute.id/index.php/al-dalil/article/view/777.

[13] Syahriati Fakhriah and Inayatul Mutmainnah, "Penerapan Sanksi Pidana Terhadap Kejahatan Siber: Sebuah Kajian Terhadap Perkembangan Hukum," *Journal of International Multidisciplinary Research* 2, no. 1 (2024): 470–477, https://www.researchgate.net/publication/378386576_Penerapan_Sanksi_Pidana_terhadap_Kejahatan_Siber_Sebuah_Kajian_terhadap_Perkembangan_Hukum.

cyberterrorism. Metode ini memungkinkan peneliti untuk mengeksplorasi perspektif berbagai pemangku kepentingan, termasuk pengguna internet, penegak hukum, dan ahli keamanan siber. Wawancara Mendalam yaitu melakukan wawancara dengan responden yang relevan, seperti praktisi hukum, akademisi, dan pengguna internet yang pernah mengalami atau menyaksikan tindakan *cyberterrorism*.

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif-analitis. Data dikumpulkan melalui studi kepustakaan, wawancara mendalam dengan para ahli hukum, praktisi keamanan siber, dan perwakilan dari instansi pemerintah terkait, serta analisis dokumen resmi seperti Undang-Undang No. 1 Tahun 2024, peraturan pelaksana, dan laporan kasus *cyberterrorism*. Analisis data dilakukan dengan pendekatan evaluatif, di mana efektivitas UU No. 1 Tahun 2024 dievaluasi berdasarkan beberapa indikator, seperti kejelasan peraturan, kesesuaian dengan kebutuhan penanganan *cyberterrorism*, serta implementasi dan koordinasi antarinstansi. Selain itu, penelitian ini juga membandingkan regulasi di Indonesia dengan negara lain yang dianggap berhasil dalam menangani *cyberterrorism* untuk memberikan rekomendasi yang relevan.

Metode analisis hukum akan digunakan untuk menilai ketentuan-ketentuan dalam UU ITE yang berkaitan dengan pencegahan *cyberterrorism*. Pendekatan ini juga akan mencakup analisis perbandingan dengan regulasi serupa di negara lain. Studi Literatur: Mengumpulkan dan menganalisis dokumen hukum, literatur akademis, serta laporan-laporan terkait implementasi UU ITE.

Analisis Normatif dengan Menilai kesesuaian norma-norma dalam UU ITE dengan prinsip-prinsip hukum yang berlaku serta efektivitasnya dalam mencegah tindakan *cyberterrorism*. Pengumpulan data akan dilakukan melalui sumber primer dan sekunder untuk memastikan keakuratan dan kelengkapan informasi. Data Primer: Diperoleh dari wawancara, FGD, dan survei kepada masyarakat mengenai pemahaman dan pengalaman mereka terkait UU ITE. Menggunakan dokumen resmi, laporan penelitian sebelumnya, serta data statistik terkait kasus *cyberterrorism* di Indonesia. Data yang terkumpul akan dianalisis menggunakan teknik analisis deskriptif dan analisis tematik untuk mengidentifikasi pola-pola yang muncul dari hasil wawancara dan diskusi. Langkah-langkah Analisis adalah dengan reduksi Data: Mengelompokkan informasi yang relevan berdasarkan tema-tema utama. Dalam Penyajian Data dengan Menyusun data dalam format yang mudah dipahami untuk memudahkan interpretasi, dan Verifikasi Data dengan Melakukan triangulasi dengan membandingkan

berbagai sumber data untuk memastikan validitas informasi.

Akhirnya, berdasarkan hasil analisis data, peneliti akan mengevaluasi sejauh mana UU ITE efektif dalam mencegah *cyberterrorism* di Indonesia. Evaluasi ini akan mempertimbangkan faktor-faktor seperti tingkat kesadaran masyarakat tentang kejahatan siber, respons aparat penegak hukum, serta tantangan yang dihadapi dalam implementasinya.

Dengan menggunakan metode penelitian ini, diharapkan dapat diperoleh gambaran yang jelas mengenai efektivitas Undang-Undang No. 1 Tahun 2024 dalam pencegahan *cyberterrorism* serta rekomendasi untuk perbaikan kebijakan di masa mendatang.

B. HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa efektivitas Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) dalam pencegahan *cyberterrorism* sangat bergantung pada alat dan sarana yang digunakan dalam implementasinya [14]. Alat dan sarana yang dimaksud meliputi, Teknologi Pemantauan Siber yaitu Pemerintah melalui instansi seperti Badan Siber dan Sandi Negara (BSSN) telah menggunakan perangkat pemantauan berbasis kecerdasan buatan (AI) dan analitik big data untuk mendeteksi aktivitas mencurigakan di dunia maya. Alat ini membantu dalam identifikasi ancaman potensial, seperti penyebaran propaganda radikal dan komunikasi yang berpotensi terorisme. Sistem Deteksi dan Respon Ancaman di UU ITE memberikan dasar hukum bagi penggunaan sistem deteksi dini (early warning system) yang terintegrasi dengan pusat data nasional. Sistem ini mampu memberikan peringatan dini kepada otoritas terkait untuk mencegah eskalasi ancaman, Infrastruktur Hukum Digital yaitu dengan Keberadaan portal aduan online yang dikelola oleh Kementerian Komunikasi dan Informatika (Kominfo) memungkinkan masyarakat melaporkan aktivitas siber yang mencurigakan. Sarana ini memperkuat partisipasi masyarakat dalam mendukung implementasi UU ITE. Pelatihan dan Sertifikasi Aparat Penegak Hukum Untuk memaksimalkan penggunaan alat-alat canggih, pelatihan intensif bagi aparat penegak hukum, seperti polisi siber, telah diadakan. Pelatihan ini mencakup teknik pengumpulan bukti digital, analisis data forensik, dan strategi menghadapi ancaman siber. Kemitraan dengan Penyedia Layanan Digital adalah salah satu sarana penting adalah kolaborasi dengan platform digital

[14] Muhammad Restu Arrasyiid, Stanley Muljadi Art, and Muhammad Rangga Arya Putra, "Implementation of the Electronic Information and Transaction Law on the Culture of Online Buying and Selling Transactions in Protecting Consumers," *JETISH: Journal of Education Technology Information Social Sciences and Health* 2, no. 2 (2023): 1121–1126, https://rayyanjurnal.com/index.php/jetish/article/view/812.

dan penyedia layanan internet untuk melacak dan menghapus konten yang melanggar UU ITE. Kerja sama ini memainkan peran penting dalam pencegahan penyebaran propaganda *cyberterrorism.*

Hasil penelitian menunjukkan bahwa Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) memiliki potensi untuk meningkatkan pencegahan *cyberterrorism* melalui pengintegrasian alat dan sarana berbasis asuransi siber[15]. Pendekatan ini menawarkan perlindungan tambahan bagi entitas yang rentan terhadap serangan siber, sekaligus mendorong kepatuhan pada standar keamanan informasi. Peran Asuransi Siber dalam Pencegahan *Cyberterrorism*, asuransi siber menyediakan perlindungan finansial bagi individu, perusahaan, atau institusi yang menjadi korban kejahatan siber, termasuk serangan yang mengarah pada *cyberterrorism*[16]. Dengan adanya asuransi siber, pihak-pihak yang terlibat didorong untuk memperkuat infrastruktur keamanan digital mereka agar memenuhi kriteria polis asuransi. Hal ini secara tidak langsung mendukung implementasi UU ITE dalam mencegah ancaman siber. Integrasi Regulasi dengan Standar Asuransi Siber UU ITE dapat mendorong penguatan regulasi terkait kewajiban entitas untuk memiliki polis asuransi siber, terutama bagi sektor strategis, seperti keuangan, energi, dan komunikasi. Kebijakan ini bertujuan untuk meningkatkan ketahanan infrastruktur kritis nasional terhadap serangan *cyberterrorism*. Dukungan terhadap Mitigasi dan Pemulihan, Dalam beberapa kasus, asuransi siber membantu entitas terdampak untuk pulih lebih cepat dari serangan. Dengan cakupan yang mencakup penggantian biaya pemulihan data, pelaporan hukum, dan perlindungan reputasi, asuransi siber menjadi sarana penting yang mendukung efektivitas UU ITE dalam penanganan insiden.

Pembahasannya adalah meskipun alat dan sarana ini telah diterapkan, terdapat beberapa tantangan yang menghambat efektivitas UU ITE, antara lain:

1. Keterbatasan Infrastruktur Teknologi, beberapa wilayah di Indonesia belum sepenuhnya memiliki infrastruktur teknologi yang memadai untuk mendukung implementasi alat pemantauan dan deteksi.

---

[15] Deny Haspada et al., "Mitigasi Pelanggaran Hukum Penggunaan Media Sosial Melalui Teknologi Informasi," *Jurnal Pengabdian Tri Bhakti* 5, no. 2 (2023): 94–98, https://www.researchgate.net/publication/385749069_Mitigasi_Pelanggaran_Hukum_Penggunaan_Media_Sosial_Melalui_Teknologi_Informasi.

[16] Jaafar Kadhim Jebur and Amany Tammouz Abdul Rahman, "Legal Concept of Cyber Risk Insurance Contract," *Evolutionary studies in imaginative culture* 8.2, no. 2 (2024): 169–178, https://esiculture.com/index.php/esiculture/article/view/1033.

2. Minimnya Literasi Digital, masyarakat yang belum paham tentang ancaman *cyberterrorism* sering kali menjadi target yang rentan bagi pelaku. Sarana edukasi literasi digital perlu diperluas untuk meningkatkan kesadaran dan kewaspadaan masyarakat.
3. Tumpang Tindih Kewenangan Antarinstansi, koordinasi antara BSSN, Kominfo, dan Kepolisian sering kali tidak optimal karena adanya tumpang tindih kewenangan dalam penggunaan alat dan pengambilan keputusan.

Sebagai rekomendasi, diperlukan integrasi teknologi yang lebih canggih, peningkatan kapasitas infrastruktur, serta penguatan kolaborasi antara pemerintah, sektor swasta, dan masyarakat. Langkah-langkah ini diharapkan dapat meningkatkan efektivitas UU No. 1 Tahun 2024 dalam mencegah ancaman *cyberterrorism*.

Meskipun integrasi asuransi siber dengan implementasi UU ITE menawarkan banyak keuntungan, terdapat beberapa kendala yang perlu diperhatikan, minimnya Kesadaran dan Pemahaman tentang Asuransi Siber. Banyak entitas, terutama usaha kecil dan menengah (UKM), belum memahami pentingnya asuransi siber sebagai perlindungan tambahan[17]. Hal ini disebabkan oleh rendahnya literasi terkait risiko kejahatan siber dan manfaat asuransi. Biaya Polis yang Relatif Tinggi, Asuransi siber sering kali dianggap mahal oleh perusahaan, terutama di sektor non-keuangan. Biaya yang tinggi ini menjadi salah satu faktor penghambat dalam adopsi asuransi siber secara luas.

Kesiapan Penyedia Layanan Asuransi ada beberapa penyedia layanan asuransi di Indonesia masih dalam tahap awal dalam menawarkan produk asuransi siber yang komprehensif. Hal ini membuat pilihan produk menjadi terbatas dan kurang relevan dengan kebutuhan perlindungan terhadap ancaman *cyberterrorism*. Sebagai rekomendasi, penelitian ini menyarankan beberapa langkah strategis: adalah bahwa Pemerintah perlu mendorong kerjasama dengan sektor asuransi untuk mengembangkan produk asuransi siber yang lebih terjangkau dan sesuai kebutuhan pasar. Meningkatkan literasi digital dan kesadaran akan manfaat asuransi siber melalui kampanye nasional yang melibatkan sektor publik dan swasta. Mengintegrasikan persyaratan kepemilikan asuransi siber ke dalam regulasi yang lebih luas, terutama untuk sektor strategis yang memiliki risiko tinggi terhadap *cyberterrorism*. Dengan menghubungkan implementasi UU ITE dan penggunaan asuransi siber, diharapkan dapat

[17] Rodney Adriko and Jason R C Nurse, "Cybersecurity, Cyber Insurance and Small-to-Medium-Sized Enterprises: A Systematic Review," *Information & computer security* 32, no. 5 (2024): 691–710, https://www.emerald.com/insight/content/doi/10.1108/ics-01-2024-0025/full/html.

tercipta ekosistem keamanan digital yang lebih kuat, sehingga pencegahan dan penanganan ancaman *cyberterrorism* dapat dilakukan secara lebih efektif.

Hasil penelitian menunjukkan bahwa UU No. 1 Tahun 2024 memiliki sejumlah keunggulan dalam memberikan landasan hukum yang jelas untuk penanganan *cyberterrorism*. Beberapa pasal dalam undang-undang ini berhasil mencakup aspek penting, seperti penindakan terhadap penyalahgunaan teknologi informasi dan perlindungan data pribadi. Namun, terdapat beberapa kendala yang menghambat efektivitasnya.

Pertama, implementasi UU ITE sering kali terkendala oleh kurangnya pemahaman teknis di kalangan aparat penegak hukum. Hal ini menyebabkan proses penanganan kasus *cyberterrorism* tidak berjalan optimal, terutama dalam hal pengumpulan bukti digital dan analisis data.

Kedua, koordinasi antarinstansi yang terlibat, seperti Kepolisian, Badan Siber dan Sandi Negara (BSSN), dan Kementerian Komunikasi dan Informatika, masih perlu ditingkatkan. Penelitian menemukan bahwa tumpang tindih kewenangan sering kali menghambat efisiensi penanganan kasus.

Ketiga, literasi digital masyarakat Indonesia masih rendah, sehingga upaya pencegahan *cyberterrorism* kurang efektif. Banyak individu yang tidak menyadari potensi bahaya dari aktivitas dunia maya yang tidak bertanggung jawab.

Sebagai perbandingan, regulasi di negara-negara maju, seperti Amerika Serikat dan Inggris, menunjukkan efektivitas yang lebih tinggi dalam penanganan *cyberterrorism* karena adanya integrasi teknologi canggih dan pelatihan yang intensif bagi aparat penegak hukum. Selain itu, integrasi dengan asuransi siber dapat menjadi solusi tambahan dalam mendukung implementasi UU ITE. Asuransi siber tidak hanya memberikan perlindungan finansial bagi korban kejahatan siber, tetapi juga mendorong kepatuhan entitas terhadap standar keamanan informasi. Dengan menghubungkan UU ITE dengan polis asuransi siber, entitas diharapkan lebih termotivasi untuk memperkuat sistem keamanan digital mereka.

Analisis Penerapan Undang-Undang No. 1 Tahun 2024 Berdasarkan analisis terhadap penerapan Undang-Undang No. 1 Tahun 2024, ditemukan bahwa undang-undang ini telah memberikan dasar hukum yang jelas untuk menangani tindakan *cyberterrorism* di Indonesia. Pengaturan mengenai informasi dan transaksi elektronik yang lebih ketat diharapkan dapat mempersempit ruang gerak para pelaku *cyberterrorism*.

Peningkatan Keamanan Sistem Informasi Hasil evaluasi menunjukkan bahwa sejumlah institusi yang terlibat dalam pengelolaan informasi dan transaksi elektronik telah meningkatkan langkah-langkah pengamanan sistem mereka. Namun, masih terdapat kelemahan pada beberapa sektor yang rentan terhadap serangan siber yang lebih canggih, seperti sektor pemerintahan dan keuangan.

Penyuluhan dan Pengawasan Upaya penyuluhan kepada masyarakat mengenai ancaman *cyberterrorism* dan pentingnya menjaga keamanan informasi semakin meningkat. Namun, pengawasan terhadap pelaksanaan undang-undang ini masih terbatas, terutama di daerah-daerah yang kurang mendapat perhatian pemerintah dalam hal infrastruktur digital.

Koordinasi Antar Lembaga Terdapat kemajuan dalam hal koordinasi antara lembaga pemerintah yang menangani masalah cybercrime dan *cyberterrorism*. Meskipun demikian, kerja sama dengan sektor swasta dan lembaga internasional dalam pencegahan ancaman ini masih perlu ditingkatkan.

Efektivitas Undang-Undang dalam Menanggulangi *Cyberterrorism* Undang-Undang No. 1 Tahun 2024 memiliki kontribusi penting dalam pencegahan dan penanggulangan *cyberterrorism*, terutama dalam memberikan dasar hukum yang lebih kuat untuk menindak tegas pelaku kejahatan dunia maya. Namun, penerapannya di lapangan memerlukan dukungan lebih lanjut, baik dari segi kebijakan maupun sumber daya manusia yang kompeten. Penguatan sistem keamanan informasi di berbagai sektor menjadi krusial untuk mencegah potensi ancaman.

Tantangan Implementasi di Lapangan Meskipun undang-undang ini cukup komprehensif, tantangan terbesar yang dihadapi adalah implementasi yang tidak merata. Beberapa daerah dan sektor masih kesulitan dalam menerapkan regulasi ini dengan maksimal. Keterbatasan anggaran dan kurangnya infrastruktur teknologi yang memadai di beberapa bagian negara menjadi hambatan besar.

Peran Penyuluhan dalam Meningkatkan Kesadaran Keamanan Penyuluhan yang lebih masif dan program edukasi terkait pencegahan *cyberterrorism* sangat penting untuk membangun kesadaran di kalangan masyarakat dan organisasi. Walaupun ada upaya dalam penyuluhan, tingkat pemahaman masyarakat tentang pentingnya menjaga keamanan data dan informasi masih rendah, yang membuka celah bagi potensi serangan.

Rekomendasi untuk Peningkatan Efektivitas Untuk meningkatkan efektivitas Undang-Undang No. 1 Tahun 2024, diperlukan adalah penguatan kapasitas lembaga penegak hukum

dalam mengatasi ancaman *cyberterrorism* melalui pelatihan dan penyediaan sumber daya manusia yang kompeten, pembaruan dan penguatan kerangka hukum secara berkala agar tetap relevan dengan perkembangan teknologi, kolaborasi yang lebih intensif antara sektor publik dan swasta serta lembaga internasional dalam pengawasan dan pencegahan *cyberterrorism*. Pengalokasian anggaran yang lebih besar untuk meningkatkan infrastruktur digital dan keamanan dunia maya, terutama di daerah-daerah yang masih tertinggal.

Secara keseluruhan, meskipun Undang-Undang No. 1 Tahun 2024 telah menunjukkan efektivitas dalam beberapa aspek, masih ada banyak ruang untuk perbaikan, terutama dalam hal implementasi dan koordinasi antar pihak yang terlibat.

C. KESIMPULAN

Penelitian ini menyimpulkan bahwa efektivitas UU No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dalam pencegahan *cyberterrorism* dapat ditingkatkan dengan mengintegrasikan penggunaan alat dan sarana, serta dukungan asuransi siber. Alat dan sarana, seperti teknologi pemantauan siber, sistem deteksi dini, dan portal pengaduan online, telah memberikan kontribusi signifikan dalam mendeteksi dan mencegah ancaman *cyberterrorism*. Namun, tantangan dalam hal infrastruktur, literasi digital, dan koordinasi antarinstansi masih perlu diatasi. Asuransi siber menjadi pelengkap yang strategis untuk meningkatkan efektivitas UU ITE. Dengan memberikan insentif kepada entitas yang mematuhi standar keamanan, asuransi siber dapat mendorong penguatan infrastruktur digital dan kesadaran akan pentingnya perlindungan terhadap ancaman siber. Untuk memastikan efektivitas maksimal, diperlukan upaya kolaboratif antara pemerintah, sektor swasta, dan masyarakat dalam mengimplementasikan UU ITE dan mengintegrasikan solusi asuransi siber ke dalam ekosistem keamanan digital nasional.

Undang-Undang No. 1 Tahun 2024 memberikan kerangka hukum yang kuat dalam menangani ancaman *cyberterrorism* dengan menyasar berbagai aktivitas ilegal di dunia maya. Meskipun telah diatur secara rinci, implementasi di lapangan masih menghadapi tantangan teknis dan administratif. Undang-Undang ini memperkuat perlindungan terhadap data pribadi dan sistem informasi, yang menjadi sasaran utama dalam serangan *cyberterrorism*. Penerapan regulasi ini diharapkan dapat meminimalisir dampak negatif dari serangan terhadap infrastruktur penting. Beberapa kendala seperti kurangnya sumber daya manusia yang terlatih, serta perbedaan interpretasi terhadap beberapa klausul hukum, mempengaruhi

efektivitas pelaksanaan undang-undang. Penyuluhan dan pelatihan terkait dengan aspek teknis dan hukum sangat diperlukan. Efektivitas pencegahan *cyberterrorism* akan meningkat jika ada sinergi antara berbagai lembaga pemerintah, sektor swasta, dan masyarakat dalam melaksanakan pengawasan dan penegakan hukum terkait dunia maya. Diperlukan penguatan kapasitas lembaga penegak hukum dan peningkatan koordinasi antar negara untuk mengatasi *cyberterrorism* secara global. Selain itu, perlu ada pembaruan berkala terhadap undang-undang agar tetap relevan dengan perkembangan teknologi informasi.

DAFTAR PUSTAKA

Adriko, Rodney, and Jason R C Nurse. "Cybersecurity, Cyber Insurance and Small-to-Medium-Sized Enterprises: A Systematic Review." *Information & computer security* 32, no. 5 (2024): 691–710. https://www.emerald.com/insight/content/doi/10.1108/ics-01-2024-0025/full/html.

Arrasyiid, Muhammad Restu, Stanley Muljadi Art, and Muhammad Rangga Arya Putra. "Implementation of the Electronic Information and Transaction Law on the Culture of Online Buying and Selling Transactions in Protecting Consumers." *JETISH: Journal of Education Technology Information Social Sciences and Health* 2, no. 2 (2023): 1121–1126. https://rayyanjurnal.com/index.php/jetish/article/view/812.

Budiman, Ahmad, Aryojati Ardipandanto, Aulia Fitri, and Siti Chaerani Dewanti. *Pembangunan Kekuatan Minimum Komponen Utama Pertahanan Negara Di Era New Normal*. Jakarta: Publica Indonesia Utama, 2021.

Dinda, Adinda Lola Sariani. "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia." *AL-DALIL: Jurnal Ilmu Sosial, Politik, dan Hukum* 2, no. 2 (2024): 69–77. https://ejournal.indrainstitute.id/index.php/al-dalil/article/view/777.

Fakhriah, Syahriati, and Inayatul Mutmainnah. "Penerapan Sanksi Pidana Terhadap Kejahatan Siber: Sebuah Kajian Terhadap Perkembangan Hukum." *Journal of International Multidisciplinary Research* 2, no. 1 (2024): 470–477. https://www.researchgate.net/publication/378386576_Penerapan_Sanksi_Pidana_terhadap_Kejahatan_Siber_Sebuah_Kajian_terhadap_Perkembangan_Hukum.

Ginting, Philemon. "Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana." Program Sarjana Universitas Diponegoro, 2008.

Haspada, Deny, Amras Mauluddin, Dimas Zulfa Santana, and Wildan Kusnaedi. "Mitigasi Pelanggaran Hukum Penggunaan Media Sosial Melalui Teknologi Informasi." *Jurnal Pengabdian Tri Bhakti* 5, no. 2 (2023): 94–98. https://www.researchgate.net/publication/385749069_Mitigasi_Pelanggaran_Hukum_Penggunaan_Media_Sosial_Melalui_Teknologi_Informasi.

Hirawan, Fajar B. *Indonesia Dan Covid-19: Pandangan Multi Aspek Dan Sektoral*. Jakarta: Centre for Strategic and International Studies, 2020.

Jebur, Jaafar Kadhim, and Amany Tammouz Abdul Rahman. "Legal Concept of Cyber Risk Insurance Contract." *Evolutionary studies in imaginative culture* 8.2, no. 2 (2024): 169–178. https://esiculture.com/index.php/esiculture/article/view/1033.

Muchamad, Masduki Khamdan, and others. *Kejahatan Siber Ancaman Dan Permasalahannya: Tinjauan Yuridis Pada Upaya Pencegahan Dan Pemberantasannya Di Indonesia*. Banda Aceh: Syiah Kuala University Press, 2023.

Mutia, Fitri, Imam Yuadi, Indy Murwindya, Ratih Wijayaningsih, Trilastiti Suryaningtyas, Wiwik Tri Yuliani, Sri Ambarwati, Bertha Niken Ayu Pratiwi, Nur Khalisha Syamsi, and Ajeng Mustika Pratiwi. *Bunga Rampai Literasi Dan Perpustakaan Berbasis Inklusi Sosial*. Sidoarjo: Zifatama Jawara, 2024.

Najwa, Amanda Fitria, and Aqila Husna. "Efektifitas Yurisdiksi Cybercrime Di Tengah Perkembangan Teknologi Informasi." *Jurnal Hukum dan Sosial Politik* 2, no. 3 (2024): 126–135. https://ifrelresearch.org/index.php/jhsp-widyakarya/article/view/3426.

Paminto, Saptaning Ruju. "Cyber Terrorism Countermeasures in Indonesia." *Jurnal Wawasan Yuridika* 6, no. 2 (2022): 186–196. https://ejournal.sthb.ac.id/index.php/jwy/article/download/464/226.

Paminto, Saptaning Ruju, Mia Amalia, Aji Mulyana, and Alika Hania Auliya. "Peran Hukum Dalam Melindungi Korban Penipuan Media Sosial Perspektif Sosiologi." *Journal Customary Law* 2, no. 1 (2024): 1–18. https://journal.pubmedia.id/index.php/jcl/article/view/3335.

Sangalang, Rizki Setyobowo, M H SH, S H Thea Farina, M Kn, and others. "Hukum Pidana Cyber: Buku Referensi." Medan: PT. Media Penerbit Indonesia, 2024.