Jurnal Review Pendidikan dan Pengajaran
http://journal.universitaspahlawan.ac.id/index.php/jrpp
Volume 7 Nomor 2, 2024
P-2655-710X e-ISSN 2655-6022

Submitted : 29/04/2024
Reviewed : 01/05/2024
Accepted : 12/05/2024
Published : 16/05/2024

Elza Qorina Pangestika [1]
Nining Suningrat[2]
Herwantono[3]
Widyastuti Andriyani[4]
Rifky Lana Rahardian[5]

PENERAPAN PRINSIP HUKUM INTERNASIONAL DALAM PENEGAKAN HUKUM TERHADAP KEJAHATAN SIBER DAN SERANGAN SIBER

Abstrak

Penelitian ini bertujuan untuk menganalisis penerapan prinsip hukum internasional dalam penegakan hukum terhadap kejahatan siber dan serangan siber. Kejahatan siber dan serangan siber merupakan ancaman serius yang terus berkembang seiring dengan kemajuan teknologi informasi. Dengan menggunakan metode studi literatur, penelitian ini mengkaji berbagai sumber, termasuk jurnal akademik, buku, dokumen kebijakan, dan laporan organisasi internasional, untuk memahami bagaimana prinsip-prinsip hukum internasional seperti kedaulatan, non-intervensi, dan kerja sama internasional diterapkan dalam konteks ini. Hasil penelitian menunjukkan bahwa Konvensi Budapest tentang Kejahatan Siber memainkan peran penting dalam membentuk kerangka hukum internasional untuk penanganan kejahatan siber. Namun, terdapat berbagai tantangan dalam implementasinya, termasuk kesenjangan kapasitas antara negara maju dan berkembang, perbedaan regulasi, dan kepentingan nasional yang beragam. Penelitian ini juga menemukan bahwa kerja sama internasional yang lebih erat dan harmonisasi hukum dapat meningkatkan efektivitas penegakan hukum siber. Sebagai saran, penelitian ini merekomendasikan peningkatan kerja sama internasional melalui perjanjian bilateral dan multilateral, pengembangan kapasitas teknologi di negara berkembang, dan partisipasi aktif sektor swasta. Upaya-upaya ini diharapkan dapat memperkuat respons global terhadap ancaman siber dan memastikan keamanan siber yang lebih baik.

Kata Kunci: Kejahatan Siber, Hukum Internasional, Penegakan Hukum

Abstact

This study aims to analyze the application of international law principles in the enforcement of laws against cybercrime and cyber attacks. Cybercrime and cyber attacks are serious threats that continue to evolve with advances in information technology. Using the literature review method, this research examines various sources, including academic journals, books, policy documents, and international organization reports, to understand how international law principles such as sovereignty, non-intervention, and international cooperation are applied in this context. The findings indicate that the Budapest Convention on Cybercrime plays a crucial role in shaping the international legal framework for addressing cybercrime. However, several challenges exist in its implementation, including capacity gaps between developed and developing countries, regulatory differences, and diverse national interests. The study also finds that closer international cooperation and legal harmonization can enhance the effectiveness of

[1]Program Studi Hukum, Fakultas Hukum, Universitas Widya Mataram
[2]Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Nahdlatul Ulama Cirebon
[3]Program Studi Teknik Sistem Perkapalan, Fakultas Teknologi Kelautan dan Perikanan, Universitas Nahdlatul Ulama Cirebon
[4]Program Studi Magister Teknologi Informasi, Fakultas Teknologi Informasi, Universitas Teknologi Digital Indonesia
[5]Program Studi Sistem Komputer, Fakultas Informatika dan Komputer, Institut Teknologi dan Bisnis STIKOM Bali
e-mail: elzaqorina20@gmail.com[1], nsuningrat23@gmail.com[2], herwantonotono944@gmail.com[3], widya@utdi.ac.id[4], rifky@stikom-bali.ac.id[5]

cyber law enforcement. As recommendations, the study suggests strengthening international cooperation through bilateral and multilateral agreements, developing technological capacity in developing countries, and active participation of the private sector. These efforts are expected to strengthen the global response to cyber threats and ensure better cybersecurity.
Keyword: Cybercrime, International Law, Law Enforcement

PENDAHULUAN

Di era digital yang semakin maju, penggunaan teknologi informasi dan komunikasi telah berkembang pesat, membawa manfaat signifikan bagi masyarakat global. Namun, kemajuan ini juga menimbulkan tantangan baru, termasuk meningkatnya insiden kejahatan siber dan serangan siber (Fahamsyah et al., 2022). Kejahatan siber mencakup berbagai aktivitas ilegal yang menggunakan komputer, jaringan, atau perangkat digital lainnya sebagai sarana atau target. Sementara itu, serangan siber merujuk pada tindakan yang bertujuan merusak, mengganggu, atau mendapatkan akses tidak sah ke sistem informasi atau data. Dalam konteks ini, penegakan hukum terhadap kejahatan siber dan serangan siber menjadi prioritas penting bagi negara-negara di seluruh dunia (Ibrahim & Triadi, 2024). Namun, sifat transnasional dari kejahatan ini menimbulkan kompleksitas dalam penanganannya. Kejahatan siber sering kali melibatkan pelaku yang beroperasi di berbagai yurisdiksi, menyulitkan proses investigasi dan penuntutan. Selain itu, perbedaan dalam sistem hukum dan regulasi antar negara menambah tantangan dalam koordinasi penegakan hukum internasional.

Prinsip hukum internasional memainkan peran krusial dalam menjembatani kesenjangan ini. Prinsip-prinsip seperti kedaulatan, non-intervensi, dan kerja sama internasional harus diterapkan secara efektif untuk menangani kejahatan siber. Kerangka hukum internasional yang ada, termasuk Konvensi Budapest tentang Kejahatan Siber, memberikan panduan bagi negara-negara dalam mengadopsi langkah-langkah legislasi dan penegakan hukum yang seragam (Fadhillah et al., 2023). Konvensi ini mendorong negara-negara untuk memperbarui undang-undang domestik mereka, meningkatkan kerja sama internasional dalam investigasi, serta berbagi informasi dan bukti yang relevan. Meskipun demikian, implementasi prinsip hukum internasional dalam penegakan hukum terhadap kejahatan siber menghadapi sejumlah tantangan. Salah satunya adalah kesenjangan kapasitas antara negara-negara maju dan berkembang dalam hal infrastruktur teknologi dan sumber daya manusia (Chotimah et al., 2019). Negara-negara berkembang sering kali mengalami kesulitan dalam mengadopsi teknologi baru dan membangun kapasitas yang diperlukan untuk menanggulangi kejahatan siber secara efektif. Selain itu, adanya perbedaan interpretasi dan penerapan prinsip hukum internasional di berbagai yurisdiksi dapat menghambat upaya koordinasi global.

Untuk mengatasi tantangan ini, diperlukan upaya kolaboratif yang melibatkan berbagai pemangku kepentingan, termasuk pemerintah, sektor swasta, dan masyarakat sipil. Pertukaran pengetahuan, pelatihan, dan pembangunan kapasitas harus ditingkatkan untuk memastikan bahwa semua negara memiliki kemampuan yang memadai dalam menangani kejahatan siber (Ariyaningsih et al., 2023). Selain itu, pengembangan kebijakan dan regulasi yang responsif terhadap dinamika teknologi juga menjadi kunci dalam memastikan bahwa penegakan hukum tetap efektif dalam menghadapi ancaman siber yang terus berkembang. Dengan demikian, penelitian ini berupaya untuk mengeksplorasi lebih dalam mengenai bagaimana prinsip-prinsip hukum internasional dapat diterapkan dalam penegakan hukum terhadap kejahatan siber dan serangan siber. Penelitian ini juga akan menyoroti tantangan dan peluang dalam mengimplementasikan kerangka hukum internasional tersebut, serta memberikan rekomendasi bagi peningkatan kerja sama internasional dalam menghadapi kejahatan siber.

METODE

Penelitian ini menggunakan metode studi literatur, yang merupakan pendekatan untuk mengumpulkan dan menganalisis informasi dari berbagai sumber tertulis yang relevan dengan topik yang diteliti (Sugiyono, 2018). Metode ini bertujuan untuk memahami dan merangkum pengetahuan yang ada, mengidentifikasi kesenjangan dalam literatur, serta memberikan dasar teoritis dan empiris untuk penelitian lebih lanjut. Berikut adalah tahapan rinci dalam penelitian ini:

1. Perumusan Pertanyaan Penelitian

Langkah awal dalam studi literatur adalah merumuskan pertanyaan penelitian yang jelas dan spesifik. Pertanyaan ini akan menjadi panduan utama dalam proses pengumpulan dan analisis literatur. Dalam konteks penelitian ini, pertanyaan utamanya adalah:

a. Bagaimana prinsip-prinsip hukum internasional diterapkan dalam penegakan hukum terhadap kejahatan siber dan serangan siber?
b. Apa saja tantangan dan peluang dalam penerapan prinsip-prinsip tersebut?

2. Identifikasi Sumber Literasi

Tahap selanjutnya adalah mengidentifikasi sumber-sumber literatur yang relevan. Sumber-sumber ini mencakup:

a. Jurnal akademik: Artikel dari jurnal hukum, teknologi informasi, dan studi keamanan siber.
b. Buku: Buku teks dan referensi yang membahas hukum internasional dan kejahatan siber.
c. Dokumen kebijakan dan regulasi: Konvensi, perjanjian internasional, undang-undang nasional, serta dokumen kebijakan terkait.
d. Laporan organisasi internasional: Laporan dari organisasi seperti Perserikatan Bangsa-Bangsa (PBB), International Telecommunication Union (ITU), dan European Union Agency for Cybersecurity (ENISA).
e. Artikel berita dan publikasi media: Artikel yang memberikan konteks dan perkembangan terbaru terkait kejahatan siber.

3. Pencarian dan Pengumpulan Data

Menggunakan kata kunci yang relevan seperti "cybercrime," "cyber attacks," "international law," "law enforcement," dan "cybersecurity cooperation," peneliti akan mencari literatur melalui database akademik (misalnya, Google Scholar, JSTOR, dan ProQuest), perpustakaan digital, dan situs web resmi organisasi internasional. Penting untuk memastikan bahwa sumber yang dikumpulkan bersifat up-to-date dan kredibel.

4. Evaluasi dan Seleksi Literatur

Setelah mengumpulkan sejumlah besar literatur, langkah berikutnya adalah mengevaluasi relevansi dan kualitas dari setiap sumber. Kriteria evaluasi meliputi:

a. Relevansi: Apakah sumber tersebut secara langsung terkait dengan topik penelitian?
b. Kredibilitas: Apakah penulis atau penerbit memiliki reputasi yang baik dalam bidangnya?
c. Tahun publikasi: Apakah informasi tersebut masih berlaku dan relevan dengan perkembangan terbaru?

Sumber-sumber yang memenuhi kriteria ini akan dipilih untuk dianalisis lebih lanjut.

5. Analisis dan Sintesis Data

Pada tahap ini, peneliti akan membaca secara mendalam setiap sumber yang telah dipilih, mencatat poin-poin penting, konsep utama, dan temuan yang relevan. Teknik analisis tematik dapat digunakan untuk mengidentifikasi tema-tema utama dan subtema yang muncul dari literatur. Langkah ini mencakup:

a. Mengelompokkan informasi: Mengelompokkan temuan berdasarkan tema, seperti penerapan prinsip kedaulatan, tantangan dalam kerja sama internasional, atau contoh kasus konkret penegakan hukum terhadap kejahatan siber.
b. Menyintesis informasi: Mengintegrasikan informasi dari berbagai sumber untuk memberikan gambaran yang komprehensif tentang topik penelitian.

6. Penyusunan Hasil dan Pembahasan

Hasil analisis akan disusun dalam bentuk narasi yang terstruktur, menjawab pertanyaan penelitian utama dan subpertanyaan. Pembahasan akan mencakup:

a. Ringkasan temuan utama: Menggambarkan bagaimana prinsip-prinsip hukum internasional diterapkan dalam penegakan hukum siber.
b. Identifikasi tantangan dan peluang: Menyoroti hambatan dan kesempatan dalam penerapan prinsip-prinsip tersebut.
c. Rekomendasi: Memberikan saran untuk meningkatkan efektivitas penegakan hukum terhadap kejahatan siber di tingkat internasional.

7. Kesimpulan

Bagian akhir dari penelitian ini adalah kesimpulan yang merangkum temuan utama, mengkonfirmasi atau menolak hipotesis awal, dan memberikan wawasan tentang implikasi penelitian bagi teori dan praktik hukum internasional.

HASIL DAN PEMBAHASAN

Berikut adalah hasil penelitian tentang penerapan prinsip hukum internasional dalam penegakan hukum terhadap kejahatan siber dan serangan siber berdasarkan metode studi literatur:

1. Penerapan Prinsip Kedaulatan dan Non-Intervensi

Penelitian ini menemukan bahwa prinsip kedaulatan dan non-intervensi tetap menjadi fondasi dalam penegakan hukum internasional terhadap kejahatan siber. Negara-negara memiliki hak kedaulatan atas ruang siber mereka, yang mencakup hak untuk mengatur dan menegakkan hukum di dalam batas yurisdiksi mereka sendiri. Namun, penerapan prinsip ini menjadi kompleks ketika kejahatan siber melibatkan pelaku atau infrastruktur di luar yurisdiksi negara yang terkena dampak. Beberapa kasus menunjukkan bahwa negara sering kali menghadapi kesulitan dalam meminta bantuan hukum dari negara lain, terutama jika hubungan diplomatik tidak harmonis (Setiawan et al., 2020)

2. Peran Kerangka Hukum Internasional

Kerangka hukum internasional, seperti Konvensi Budapest tentang Kejahatan Siber, berperan penting dalam memfasilitasi kerja sama internasional. Konvensi ini memberikan panduan komprehensif bagi negara-negara dalam merumuskan undang-undang domestik terkait kejahatan siber dan menetapkan mekanisme untuk kerja sama lintas batas. Studi literatur menunjukkan bahwa negara-negara yang telah mengadopsi Konvensi Budapest cenderung memiliki sistem penegakan hukum yang lebih kuat dan efektif dalam menangani kejahatan siber (Mustameer, 2022).

3. Tantangan dalam Penegakan Hukum Siber

Analisis literatur mengidentifikasi beberapa tantangan utama dalam penegakan hukum terhadap kejahatan siber (Farhan et al., 2023):

a. Kesenjangan Kapasitas: Negara-negara berkembang sering kali kekurangan infrastruktur teknologi dan sumber daya manusia yang memadai untuk menangani kejahatan siber secara efektif. Kesenjangan ini menghambat upaya global dalam melawan kejahatan siber.
b. Perbedaan Hukum dan Regulasi: Variasi dalam undang-undang dan regulasi antara negara-negara membuat koordinasi penegakan hukum menjadi sulit. Misalnya, tindakan yang dianggap ilegal di satu negara mungkin tidak diakui sebagai pelanggaran di negara lain.
c. Kepentingan Nasional yang Berbeda: Negara-negara mungkin memiliki prioritas yang berbeda dalam hal keamanan siber, yang dapat menghambat upaya kerja sama internasional. Beberapa negara mungkin lebih fokus pada perlindungan data pribadi, sementara yang lain lebih menekankan pada keamanan nasional.

4. Peluang dalam Kerja Sama Internasional

Meskipun terdapat banyak tantangan, studi literatur juga mengungkapkan berbagai peluang untuk meningkatkan kerja sama internasional dalam penegakan hukum terhadap kejahatan siber (Nabila et al., 2024):

a. Pengembangan Kapasitas: Inisiatif internasional untuk meningkatkan kapasitas teknologi dan sumber daya manusia di negara-negara berkembang dapat memperkuat upaya global dalam menangani kejahatan siber. Program pelatihan dan pertukaran pengetahuan antara negara-negara maju dan berkembang sangat penting.
b. Harmonisasi Hukum: Upaya untuk menyelaraskan undang-undang dan regulasi terkait kejahatan siber di berbagai negara dapat memfasilitasi kerja sama penegakan hukum lintas batas. Harmonisasi ini dapat dicapai melalui perjanjian internasional dan konvensi.
c. Pembentukan Alat dan Mekanisme Baru: Pembentukan mekanisme baru, seperti pusat koordinasi internasional untuk respons terhadap insiden siber, dapat membantu

mengatasi tantangan dalam koordinasi penegakan hukum. Mekanisme ini dapat menyediakan platform untuk berbagi informasi, mengoordinasikan investigasi, dan mengembangkan strategi bersama.

Di era digital ini, teknologi informasi dan komunikasi telah menjadi bagian integral dari kehidupan sehari-hari, mendorong transformasi dalam berbagai sektor seperti ekonomi, pendidikan, dan pemerintahan. Namun, seiring dengan manfaatnya, muncul tantangan baru berupa kejahatan siber dan serangan siber yang semakin kompleks dan transnasional. Kejahatan siber, yang mencakup aktivitas ilegal melalui komputer dan jaringan, serta serangan siber yang bertujuan merusak atau mencuri data, menuntut respons hukum yang efektif dan terkoordinasi secara global (Wicaksana et al., 2020). Dalam konteks ini, penerapan prinsip hukum internasional menjadi sangat krusial.

Prinsip kedaulatan negara adalah salah satu pilar utama hukum internasional yang harus diperhatikan dalam penanganan kejahatan siber. Kedaulatan memberikan hak kepada setiap negara untuk mengatur dan menegakkan hukum di wilayah yurisdiksinya, termasuk ruang siber. Namun, ketika pelaku kejahatan siber beroperasi melintasi batas negara, penerapan prinsip kedaulatan menghadapi tantangan besar. Misalnya, sebuah serangan siber yang dilancarkan dari satu negara ke negara lain memerlukan kerja sama lintas batas untuk investigasi dan penuntutan. Prinsip non-intervensi juga relevan di sini, menuntut negara untuk tidak campur tangan dalam urusan domestik negara lain, termasuk dalam urusan siber (Salsabilla et al., 2023).

Konvensi Budapest tentang Kejahatan Siber adalah kerangka hukum internasional yang paling komprehensif dan diakui luas dalam penanggulangan kejahatan siber. Konvensi ini memberikan pedoman bagi negara-negara dalam membentuk undang-undang domestik yang sesuai, serta menetapkan mekanisme untuk kerja sama internasional dalam hal penegakan hukum (Muchamad, 2023). Penelitian menunjukkan bahwa negara-negara yang telah meratifikasi Konvensi Budapest memiliki sistem hukum yang lebih efektif dalam menangani kejahatan siber. Mereka mampu mengadopsi langkah-langkah legislasi yang seragam, memfasilitasi kerja sama internasional, dan mempercepat proses berbagi informasi dan bukti yang diperlukan untuk penuntutan.

Meskipun demikian, implementasi prinsip hukum internasional tidak terlepas dari berbagai tantangan. Salah satu tantangan terbesar adalah kesenjangan kapasitas antara negara-negara maju dan berkembang (Hastri, 2021). Negara-negara berkembang sering kali tidak memiliki infrastruktur teknologi dan sumber daya manusia yang memadai untuk menangani kejahatan siber secara efektif. Mereka membutuhkan bantuan dalam bentuk teknologi dan pelatihan untuk membangun kapasitas penegakan hukum siber yang kuat. Selain itu, perbedaan dalam sistem hukum dan regulasi antar negara menambah kompleksitas dalam koordinasi penegakan hukum internasional (Jubhari, 2022). Tindakan yang dianggap sebagai kejahatan di satu negara mungkin tidak diakui sebagai pelanggaran di negara lain, sehingga menghambat upaya kerja sama.

Kerja sama internasional menjadi kunci dalam mengatasi tantangan-tantangan tersebut. Negara-negara perlu berkolaborasi lebih erat melalui perjanjian bilateral dan multilateral, serta berpartisipasi aktif dalam organisasi internasional yang berfokus pada keamanan siber (Najwa, 2024). Pengembangan kapasitas juga harus menjadi prioritas, dengan inisiatif internasional yang bertujuan untuk meningkatkan kemampuan teknologi dan sumber daya manusia di negara-negara berkembang. Selain itu, harmonisasi hukum dan regulasi di berbagai negara dapat membantu menciptakan standar yang lebih seragam, memudahkan koordinasi dan penegakan hukum lintas batas.

Sebagai tambahan, sektor swasta juga memainkan peran penting dalam penegakan hukum siber (Maskun et al., 2020). Perusahaan teknologi dan penyedia layanan internet memiliki kemampuan untuk mendeteksi aktivitas mencurigakan dan melaporkan insiden siber secara real-time. Kolaborasi antara pemerintah dan sektor swasta dapat mempercepat respons terhadap serangan siber dan meminimalisir dampaknya (Herera & Sebyar, 2023). Pengembangan kebijakan yang mendorong partisipasi aktif sektor swasta dalam keamanan siber adalah langkah yang penting. Pada akhirnya, penelitian ini menyoroti bahwa penerapan prinsip hukum internasional dalam penegakan hukum terhadap kejahatan siber dan serangan siber memerlukan

pendekatan yang holistik dan kolaboratif. Meskipun terdapat tantangan yang signifikan, terdapat pula peluang besar untuk meningkatkan efektivitas penegakan hukum melalui kerja sama internasional yang lebih erat, pengembangan kapasitas, harmonisasi hukum, dan partisipasi aktif sektor swasta (Situmeang, 2021). Dengan langkah-langkah ini, komunitas internasional dapat lebih baik melindungi ruang siber dari ancaman kejahatan dan serangan siber, serta memastikan keamanan dan stabilitas digital bagi semua negara.

SIMPULAN

Penelitian ini menyimpulkan bahwa penerapan prinsip hukum internasional dalam penegakan hukum terhadap kejahatan siber dan serangan siber adalah krusial namun kompleks. Prinsip-prinsip seperti kedaulatan, non-intervensi, dan kerja sama internasional harus diterapkan secara efektif untuk mengatasi tantangan yang timbul dari sifat transnasional kejahatan siber. Konvensi Budapest tentang Kejahatan Siber berfungsi sebagai kerangka kerja penting, meskipun kesenjangan kapasitas dan perbedaan regulasi antar negara tetap menjadi hambatan utama. Kolaborasi internasional yang lebih erat, peningkatan kapasitas teknologi, dan partisipasi aktif sektor swasta sangat diperlukan untuk meningkatkan efektivitas penegakan hukum siber.

SARAN

Penelitian ini menyarankan agar negara-negara memperkuat kerja sama internasional melalui perjanjian bilateral dan multilateral serta berpartisipasi aktif dalam organisasi internasional terkait keamanan siber. Selain itu, perlu ada upaya harmonisasi hukum dan regulasi serta peningkatan kapasitas teknologi dan sumber daya manusia, khususnya di negara-negara berkembang. Pemerintah juga harus mendorong kolaborasi dengan sektor swasta untuk respons yang lebih cepat dan efektif terhadap ancaman siber.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah mendukung penelitian ini. Terima kasih juga kepada institusi dan organisasi yang menyediakan sumber daya dan akses ke literatur yang diperlukan. Dukungan Anda semua sangat berarti bagi keberhasilan penelitian ini.

DAFTAR PUSTAKA

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. Justisia: Jurnal Ilmu Hukum, 1(1), 1–11.

Chotimah, H. C., Iswardhana, M. R., & Pratiwi, T. S. (2019). Penerapan Military Confi dence Building Measures dalam Menjaga Ketahanan Nasional Indonesia di Ruang Siber. Jurnal Ketahanan Nasional, 25(3), 331.

Fadhillah, S. A., Matakupan, M. S. A., & Mingga, B. W. B. (2023). Peran Interpol dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest On Cybercrimes. Journal on Education, 5(4), 16553–16564.

Fahamsyah, E., Taniady, V., Rachim, K. V., & Riwayanti, N. W. (2022). Penerapan Prinsip Aut Dedere Aut Judicare Terhadap Pelaku Cybercrime Lintas Negara Melalui Ratifikasi Budapest Convention. Jurnal Hukum Dan Syariah De Jure, 14.

Farhan, M., Syaefunaldi, R., Hidayat, D. R. D., & Hosnah, A. U. (2023). Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber. Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora, 1(6), 8–20.

Hastri, E. D. (2021). Cyber Espionage Sebagai Ancaman Terhadap Pertahanan dan Keamanan Negara Indonesia. Law & Justice Review Journal, 1(1), 12–25.

Herera, D. A., & Sebyar, M. H. (2023). Perlindungan Hukum terhadap Serangan Siber: Tinjauan Atas Kebijakan dan Regulasi Terbaru. Causa: Jurnal Hukum Dan Kewarganegaraan, 1(4), 21–30.

Ibrahim, M. A., & Triadi, I. (2024). Dinamika Hukum Pertahanan Dan Keamanan Negara Dalam Konteks Globalisasi: Tantangan Dan Prospek Di Abad Ke-21. Hakim, 2(1), 110–117.

Jubhari, A. R. (2022). Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber

Menggunakan Virus Ransomware WannaCry di Indonesia. Universitas Hasanuddin.

Maskun, S. H., LM, L., Maskun, S. H., LM, L., Achmad, S. H., MH, A. S. H., Naswar, S. H., Assidiq, A., & Lubis, S. N. (2020). Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional.

Muchamad, M. K. (2023). Kejahatan Siber Ancaman dan Permasalahannya: Tinjauan Yuridis pada Upaya Pencegahan dan Pemberantasannya di Indonesia. Syiah Kuala University Press.

Mustameer, H. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. Jurnal Yustika: Media Hukum Dan Keadilan, 25(01), 40–53.

Nabila, A. P., Manabung, N. A., & Ramadhansha, A. C. (2024). Peran Hukum Internasional Dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional. Indonesian Journal of Law, 1(1), 26–37.

Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum, 2(1), 8–16.

Salsabilla, S. A., Andiani, K., & Hosnah, A. U. (2023). Penegakan Hukum dalam Era Society 5.0: Cyber Espionage dalam Sorotan Hukum Nasional dan Internasional. Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora, 1(5), 178–191.

Setiawan, W. B. M., Churniawan, E., & Faried, F. S. (2020). Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber (Cyber Attack) Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia. Jurnal USM Law Review, 3(2), 275–295.

Situmeang, S. M. T. (2021). Penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber. Sasi, 27(1), 38–52.

Sugiyono. (2018). Metode Penelitian Evaluasi. Yogyakarta: Alfabeta.

Wicaksana, R. H., Munandar, A. I., & Samputra, P. L. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 (A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic). JURNAL IPTEKKOM Jurnal Ilmu Pengetahuan & Teknologi Informasi, 22(2), 143–158.