PERKARA
Jurnal Ilmu Hukum dan Politik

LPPM Universitas Sains dan Teknologi Komputer
Vol. 3 No. 2 Juni 2025, Hal. 860-875
E-ISSN: 2988-5213; P-ISSN: 2988-7747
https://journal.stekom.ac.id/index.php/PERKARA

The Role of Interpol in Addressing Transnational Cybercrime: A Review of Global Law Enforcement Collaboration in Southeast Asia

Dian Kharisma[1], Ni Luh Putu Erika Swandiani*[2], Andi Nur Azizah Ardan Paliwang[3]
[1] *Fakultas Hukum, Universitas Sains dan Teknologi Komputer Semarang, Jawa Tengah, Indonesia*
[2, 3] *Fakultas Hukum dan Ilmu Sosial, Universitas Pendidikan Ganesha, Bali, Indonesia*
E-mail: ni.luhputu@gmail.com

Article Info

Keywords:
Cybercrim
Interpol
Regional Cooperation
Cybersecurity
Southeast Asia

Abstract

Transnational cybercrime is emerging today as a significant new worldwide menace, and in Southeast Asia, which is undergoing rapid digitalization but is marked by varying legal and technical capabilities. This paper, therefore, seeks to examine the role of Interpol in contributing strategically to strengthening law enforcement collaboration to combat cybercrime in Southeast Asia. The approach used in this study was descriptive qualitative, particularly case studies. It involved the collection of evidence from 30 official documents, Interpol reports, and scholarly literature dated from 2019 to 2024. The findings revealed that Interpol achieves this through intelligence exchange via the I-24/7 platform, technical training, and joint operations, such as Operation Haechi and Night Fury. Notwithstanding the auspicious connotation birthed by this collaboration, the variations in national capacities, dearth in digital infrastructure, as well as differences in legal frameworks, collectively form rather significant hurdles. Accordingly, this research provides a theoretical contribution towards enhancing understanding of the institutional role in regional cybersecurity and practical contributions in suggesting measures for optimizing cooperation in ASEAN. The interdisciplinary approach employed in this study is a significant innovation in bridging the gap in the literature on the role of international organizations in the fight against transnational cybercrime.

DOI: *https://doi.org/10.51903/nrcgp489*
Submitted: April 2025, Reviewed: May 2025, Accepted: June 2025
**Corresponding Author*

I. PENDAHULUAN

Kejahatan siber telah menjadi salah satu tantangan global paling signifikan dalam dekade terakhir, terutama karena sifatnya yang lintas negara dan terus berkembang secara teknologi (Laksito et al., 2024; Zhou et al., 2024). Kejahatan ini tidak hanya menyasar individu atau entitas privat, tetapi juga berdampak luas pada sistem keamanan nasional, ekonomi digital, dan infrastruktur publik suatu negara. Di kawasan Asia Tenggara, digitalisasi ekonomi dan pertumbuhan populasi daring yang pesat telah menciptakan ruang yang rentan terhadap eksploitasi oleh jaringan kejahatan siber lintas negara (Lazarus et al., 2025). Fenomena ini menuntut adanya bentuk kerja sama internasional yang lebih terstruktur dan responsif. Dalam konteks inilah, peran Interpol sebagai organisasi penegakan hukum internasional menjadi sangat relevan. Interpol memiliki mandat global untuk memfasilitasi koordinasi antarnegara

dalam menghadapi kejahatan lintas yurisdiksi, termasuk dalam bidang siber yang kian kompleks (Ferdinan Sitompul et al., 2024). Penelitian ini muncul dari kebutuhan untuk memahami secara lebih spesifik bagaimana Interpol memainkan peran strategisnya dalam konteks kawasan Asia Tenggara yang memiliki karakteristik hukum, politik, dan kapasitas teknologi yang beragam.

Fenomena kejahatan siber lintas negara menunjukkan peningkatan secara kuantitatif dan kualitatif. Berdasarkan data dari (Ferdinan Sitompul et al., 2024), tercatat lebih dari 135.000 insiden kejahatan siber lintas negara terjadi di Asia Tenggara selama tahun 2023, dengan jenis kejahatan yang meliputi phishing, serangan ransomware, eksploitasi data pribadi, hingga infiltrasi terhadap sistem pemerintahan. Negara-negara dengan infrastruktur digital yang semakin maju seperti Singapura dan Malaysia menjadi target utama, namun negara berkembang seperti Indonesia dan Filipina juga mengalami peningkatan serangan, terutama pada sektor keuangan dan layanan publik (Ali et al., 2025). Interpol melalui Cybercrime Directorate dan ASEAN Cybercrime Operations Desk, telah menjalankan sejumlah inisiatif seperti operasi koordinatif (Operation Night Fury, Haechi), pembagian intelijen kriminal siber, dan pelatihan teknis untuk aparat penegak hukum lokal (Hongyue Jin & Guo, 2023). Namun demikian, seberapa efektif peran Interpol dalam memperkuat kerja sama penegakan hukum di kawasan ini masih belum banyak dijelaskan secara komprehensif dalam kajian akademik, meskipun signifikansinya semakin mendesak.

Tinjauan literatur menunjukkan bahwa peran organisasi internasional dalam penanganan kejahatan lintas negara telah menjadi perhatian berbagai kalangan peneliti. (Wang, 2024) menekankan pentingnya integrasi hukum internasional dalam penanggulangan kejahatan siber global. (Cieslik & Ghodsi, 2024) menyatakan bahwa ketidakharmonisan regulasi antarnegara menjadi penghambat utama dalam upaya kerja sama lintas batas. Di sisi lain, (Wilner et al, 2024) menyoroti keberhasilan beberapa operasi siber internasional yang menunjukkan efektivitas kerja sama global. Penelitian terkini dari (Khan, 2024) mengemukakan perlunya rekonstruksi strategi kepolisian siber di Singapura, yang relevan sebagai model perbandingan kelembagaan dalam kawasan . Selain itu, (Ma et al., 2024) memperlihatkan bahwa kerjasama regional menghadapi tantangan struktural yang bersifat kelembagaan, terutama dalam harmonisasi hukum dan koordinasi operasional lintas negara . Namun, mayoritas penelitian lebih menekankan pada pendekatan hukum atau teknologi semata, tanpa banyak menyentuh aspek institusional dan peran koordinatif Interpol, khususnya dalam konteks kawasan ASEAN. Ini menunjukkan bahwa masih terbatas kajian akademik yang membahas peran Interpol secara empirik dalam mengatasi kejahatan siber di wilayah dengan kepentingan geopolitik yang kompleks seperti Asia Tenggara.

Dari kajian tersebut dapat diidentifikasi adanya kesenjangan (research gap) dalam pemahaman mengenai bagaimana Interpol mengoperasionalisasikan mandatnya dalam konteks regional, serta bagaimana aktor-aktor penegakan hukum nasional merespons koordinasi tersebut. Literatur sebelumnya cenderung normatif dan bersifat global, sehingga belum mengungkapkan secara rinci dinamika

kolaborasi penegakan hukum yang melibatkan Interpol dan negara-negara Asia Tenggara (Sundram, 2024). Selain itu, belum banyak penelitian yang menganalisis hambatan implementasi di lapangan, seperti keterbatasan sumber daya, perbedaan kebijakan hukum siber antarnegara, serta ketimpangan kapasitas teknologi informasi. Gap inilah yang menjadi justifikasi utama dari penelitian ini, bahwa perlu adanya kajian yang secara spesifik menggambarkan dan menganalisis bentuk kolaborasi penegakan hukum yang dimediasi oleh Interpol, tantangan yang dihadapi, dan potensi optimalisasi ke depan.

Tujuan dari penelitian ini adalah untuk menganalisis peran Interpol dalam menangani kejahatan siber lintas negara di Asia Tenggara dengan fokus pada mekanisme kolaborasi antarpenegak hukum, tantangan operasional, serta efektivitas strategi yang dijalankan. Secara khusus, penelitian ini bertujuan mengungkap bagaimana Interpol memfasilitasi pertukaran informasi intelijen, pelatihan teknis, serta operasi terkoordinasi antaranggota ASEAN dalam menangani serangan siber transnasional (Marjun et al., 2025). Penelitian ini juga bertujuan untuk mengevaluasi respons masing-masing negara terhadap inisiatif Interpol, dan bagaimana kerangka kerja sama tersebut dapat ditingkatkan ke depannya.

Aspek kebaruan (novelty) dari penelitian ini terletak pada pendekatannya yang menyinergikan analisis kelembagaan Interpol, dinamika regional Asia Tenggara, dan kompleksitas kejahatan siber lintas batas. Penelitian ini tidak hanya menyumbang pada aspek teoritis dengan menawarkan model pemetaan peran organisasi internasional dalam kerja sama keamanan digital regional (Sachoulidou, 2024), tetapi juga memberikan kontribusi praktis berupa rekomendasi berbasis data mengenai optimalisasi kolaborasi penegakan hukum lintas negara. Berbeda dengan penelitian internasional yang banyak berfokus pada konteks global atau negara maju (misalnya model Eropa dan Amerika Utara), artikel ini menegaskan kontribusi spesifik pada konteks ASEAN, di mana kesenjangan kapasitas antarnegara lebih tajam dan koordinasi kelembagaan lebih kompleks. Dengan demikian, penelitian ini memberikan perspektif baru mengenai bagaimana peran Interpol dapat dioperasionalisasikan dalam lingkungan regional yang memiliki fragmentasi hukum, politik, dan teknologi, yang belum banyak dieksplorasi dalam literatur internasional. Dengan mengintegrasikan studi dokumenter, analisis kebijakan, dan perspektif empiris, penelitian ini menawarkan pendekatan yang komprehensif dan kontekstual, yang belum banyak ditemukan dalam literatur sebelumnya.

Signifikansi dari penelitian ini dapat dilihat dari dua sisi. Dari sisi teoritis, penelitian ini berkontribusi pada pengembangan studi hubungan internasional dan keamanan siber dengan menempatkan Interpol sebagai studi kasus organisasi internasional yang menjalankan fungsi koordinatif dalam konteks kawasan (Farber, 2025). Dari sisi praktis, hasil penelitian ini dapat menjadi masukan strategis bagi pemerintah, aparat penegak hukum, dan pembuat kebijakan di Asia Tenggara dalam merumuskan kerangka kerja sama yang lebih terintegrasi dan adaptif terhadap tantangan kejahatan siber. Penelitian ini juga bermanfaat bagi Interpol itu sendiri sebagai refleksi kelembagaan dan evaluasi terhadap efektivitas perannya di wilayah yang sangat dinamis seperti Asia Tenggara.

Sebagai landasan teoritis yang mengarahkan analisis selanjutnya, penelitian ini akan mengadopsi teori institusionalisme global (Scholte, 2021) untuk menjelaskan bagaimana aturan, norma, dan praktik global seperti yang difasilitasi oleh Interpol diadopsi, diadaptasi, dan diinternalisasi dalam sistem hukum negara ASEAN. Selain itu, teori jaringan penegakan hukum transnasional (Bekkers et al., 2025) akan digunakan untuk memahami struktur, interaksi, dan pola kolaborasi antar-aktor, serta untuk memetakan bagaimana dinamika jaringan ini mempengaruhi efektivitas respons terhadap serangan siber lintas negara. Pendekatan ganda ini akan membantu mengeksplorasi tidak hanya dimensi kelembagaan, tetapi juga aspek relasional dan operasional dalam kolaborasi lintas yurisdiksi.

II. METODOLOGI

A. Desain Penelitian

Penelitian ini mengadopsi pendekatan kualitatif deskriptif dengan strategi studi kasus, yang difokuskan pada aktivitas Interpol dalam menangani kejahatan siber antarnegara di kawasan Asia Tenggara. Pendekatan kualitatif dipilih karena sifat permasalahan yang kompleks dan menuntut eksplorasi mendalam atas interaksi kelembagaan dan dinamika kebijakan antaraktor. Penggunaan metode studi kasus memungkinkan peneliti menggali fenomena secara menyeluruh dalam batasan konteks waktu dan lokasi tertentu, yakni antara tahun 2019 hingga 2024. Tujuan utama penelitian ini bukan untuk mengeneralisasi secara statistik, melainkan memperoleh pemahaman mendalam tentang bentuk kolaborasi, strategi implementatif, serta hambatan koordinasi lintas negara yang dihadapi oleh Interpol bersama negara-negara ASEAN. Desain ini mendukung kombinasi antara analisis literatur, interpretasi kebijakan, dan eksplorasi empiris terhadap data dokumen resmi.

B. Populasi dan Sampel

Subjek utama dalam penelitian ini mencakup beragam dokumen seperti laporan tahunan Interpol, kebijakan kerja sama regional ASEAN, artikel ilmiah internasional, dan pemberitaan media kredibel yang berkaitan dengan kolaborasi penegakan hukum siber di Asia Tenggara. Pengambilan sampel dilakukan dengan teknik purposive sampling, di mana hanya dokumen yang memenuhi kriteria tertentu yang diseleksi, yakni: (1) membahas peran Interpol dalam konteks siber, (2) terbit dalam kurun 2019–2024, (3) berhubungan langsung dengan kawasan ASEAN, dan (4) berasal dari sumber resmi atau jurnal ilmiah terpercaya. Total terdapat sekitar 30 dokumen utama yang digunakan dalam analisis, yang mewakili kompleksitas hubungan antar lembaga penegakan hukum serta kerangka kerja Interpol di wilayah Asia Tenggara.

C. Prosedur Pengumpulan Data

Proses pengumpulan data dilakukan melalui pengkajian dokumen serta literatur ilmiah, dengan tahapan yang sistematis. Awalnya, peneliti mengakses dan mengumpulkan dokumen resmi dari situs Interpol, lembaga regional ASEAN, dan badan penegak hukum nasional, mencakup laporan kegiatan, operasi siber, serta program pelatihan. Kemudian, artikel ilmiah dipilih dari database akademik seperti Scopus,

JSTOR, dan Google Scholar dengan penggunaan kata kunci yang relevan. Setelah dikumpulkan, dokumen-dokumen tersebut disortir berdasarkan keterkaitan tematik dan dianalisis menggunakan kerangka analisis awal. Untuk menjaga transparansi, validasi data dilakukan melalui triangulasi sumber, yakni membandingkan dokumen resmi Interpol dengan laporan akademik dan publikasi media kredibel. Selain itu, proses pemilihan dokumen menggunakan kriteria relevansi dan keandalan, dengan tahapan peer debriefing bersama pakar hukum siber guna memastikan objektivitas seleksi. Langkah ini memberikan justifikasi metodologis bahwa data yang dianalisis tidak hanya representatif, tetapi juga memenuhi standar validitas akademik. Pengumpulan ini berlangsung selama tiga bulan dan dilaksanakan secara konsisten untuk menjamin keakuratan dan keluasan informasi yang diperoleh dalam menjawab fokus penelitian.

D. Instrumen Penelitian

Alat utama yang digunakan dalam penelitian ini berupa lembar kategorisasi tematik yang dirancang berdasarkan dua kerangka teori, yaitu teori institusionalisme global dan teori jaringan penegakan hukum lintas negara. Instrumen ini membantu proses klasifikasi konten dokumen ke dalam beberapa kategori penting seperti bentuk kerja sama Interpol, tantangan struktural regional, tingkat efektivitas pelaksanaan, serta respons masing-masing negara anggota ASEAN. Instrumen ini diuji secara terbatas pada lima dokumen awal untuk mengukur konsistensi penerapan kode. Hasil uji menunjukkan bahwa instrumen memiliki tingkat ketelitian yang baik dan sesuai untuk menangkap elemen-elemen penting dalam dinamika kolaborasi penegakan hukum yang dikaji.

E. Prosedur Analisis Data

Tahapan analisis data dilakukan dengan metode analisis isi tematik, dibantu oleh perangkat lunak NVivo versi 14. Analisis diawali dengan penyusunan data secara sistematik, kemudian pemberian kode tematik terhadap bagian teks yang dianggap signifikan. Kode-kode tersebut lalu dikelompokkan ke dalam tema utama seperti "kerja sama operasional Interpol", "tantangan hukum dan kelembagaan", serta "respon kebijakan negara ASEAN". Proses interpretasi dilakukan untuk memahami hubungan antar tema dan menyusun narasi atas temuan. Untuk menjaga validitas, dilakukan triangulasi antar sumber dan proses diskusi dengan pakar (peer debriefing) guna memastikan ketepatan interpretasi. Dengan pendekatan ini, analisis berjalan secara mendalam dan kontekstual.

F. Langkah-Langkah Pelaksanaan

Pelaksanaan penelitian terdiri dari beberapa tahap penting. Tahap awal dimulai dengan penyusunan desain konseptual serta kerangka teori sebagai landasan analisis. Langkah berikutnya adalah pengumpulan dan seleksi data, yang meliputi pencarian dokumen dan artikel yang sesuai dengan fokus penelitian. Setelah data terkumpul, proses dilanjutkan dengan pengkodean dan analisis tematik menggunakan perangkat lunak NVivo untuk mengidentifikasi pola-pola utama. Akhirnya, peneliti menyusun kesimpulan dan rekomendasi kebijakan berdasarkan hasil analisis. Seluruh proses ini

dilaksanakan dalam kurun waktu lima bulan, dengan penekanan pada sistematika kerja dan ketelitian dalam setiap tahapan.

G. Pertimbangan Etis

Walaupun penelitian ini tidak melibatkan subjek manusia secara langsung, aspek etika tetap dijaga secara ketat. Peneliti memastikan seluruh sumber dikutip secara akurat dan sesuai dengan kaidah ilmiah. Selain itu, seluruh dokumen yang digunakan adalah dokumen publik, sehingga tidak terdapat risiko pelanggaran terhadap data rahasia atau informasi sensitif institusional. Objektivitas dalam analisis dijaga melalui penyusunan laporan yang transparan, serta tidak melakukan manipulasi terhadap isi dokumen. Jika nantinya dibutuhkan untuk keperluan publikasi ilmiah, maka prosedur persetujuan etik institusional akan diajukan sesuai standar akademik yang berlaku.

III. HASIL DAN DISKUSI

Hasil

A. Penyajian Data Hasil Penelitian

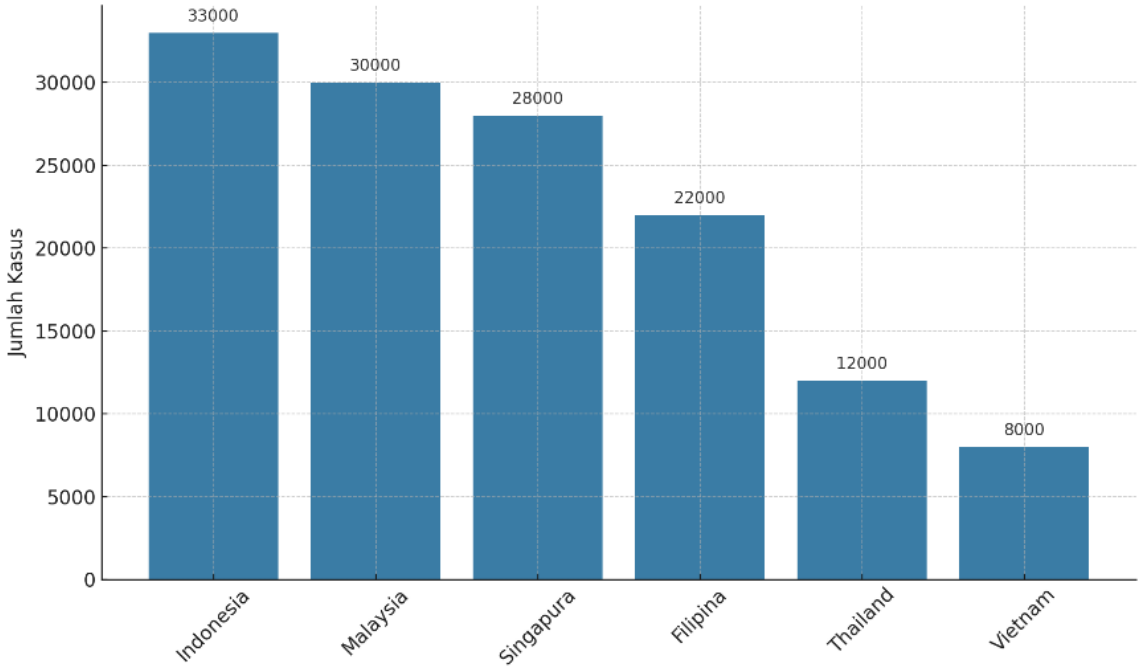
Penelitian ini berhasil menghimpun berbagai data dan temuan utama dari 30 dokumen resmi, laporan tahunan, dan publikasi ilmiah antara tahun 2019 hingga 2024. Fokus utama diarahkan pada inisiatif Interpol dalam menangani kejahatan siber lintas negara di kawasan Asia Tenggara. Dari pengumpulan tersebut, teridentifikasi sejumlah inisiatif penting, seperti Operation Haechi, ASEAN Cybercrime Desk, Operation Night Fury, serta program pelatihan teknis untuk aparat penegak hukum. Rincian dapat dilihat dalam Tabel 1. Beberapa dari inisiatif tersebut telah dilaksanakan secara berkelanjutan dan menunjukkan peningkatan dalam kolaborasi antarnegara.

Tabel 1. Inisiatif Utama Interpol dalam Penanganan Kejahatan Siber di Asia Tenggara (2019–2024)

No	Inisiatif / Operasi	Tahun	Negara Terlibat	Bentuk Kegiatan
1	Operation Haechi	2021–2024	Indonesia, Malaysia, Filipina	Penindakan penipuan daring lintas negara
2	ASEAN Cybercrime Desk	Sejak 2019	Semua negara ASEAN	Fasilitasi koordinasi dan pertukaran intelijen
3	Operation Night Fury	2023	Singapura, Vietnam	Penindakan ransomware dan malware
4	Pelatihan Cybercrime INTERPOL	2020–2024	Indonesia, Thailand	Pelatihan teknis investigasi digital

Data dari INTERPOL (2024) menunjukkan distribusi insiden kejahatan siber yang tinggi di Asia Tenggara, dengan konsentrasi terbesar di Indonesia, Malaysia, dan Singapura. Gambar 1 menampilkan jumlah insiden kejahatan siber lintas negara sepanjang tahun 2023 di enam negara anggota ASEAN. Indonesia mencatat 33.000 insiden, disusul Malaysia (30.000), Singapura (28.000), Filipina (22.000), Thailand (12.000), dan Vietnam (8.000). Negara dengan populasi daring besar dan infrastruktur digital lebih maju cenderung menjadi target utama. Perbedaan kesiapan siber dan penegakan hukum turut memengaruhi tingkat pelaporan dan deteksi insiden. Jika dibandingkan antarnegara ASEAN, terlihat adanya ketimpangan signifikan dalam kapasitas penegakan hukum. Singapura dan Malaysia, dengan

infrastruktur digital lebih maju, menunjukkan tingkat keterlibatan lebih tinggi dalam operasi terkoordinasi. Sebaliknya, negara seperti Laos, Myanmar, dan Kamboja masih memiliki keterbatasan baik dari sisi teknis maupun kelembagaan. Ketimpangan ini menegaskan bahwa keberhasilan kolaborasi regional sangat bergantung pada kemampuan Interpol untuk menjembatani kesenjangan kapasitas, sehingga tidak terjadi "asymmetric burden" dalam strategi penanggulangan kejahatan siber. Temuan ini menegaskan bahwa strategi kolaboratif regional yang adaptif terhadap dinamika ancaman digital sangat dibutuhkan.



Gambar 1. Distribusi Kasus Kejahatan Siber Lintas Negara di Asia Tenggara (2023)

Untuk memberikan gambaran yang lebih ringkas mengenai variasi keterlibatan negara-negara ASEAN dalam kerja sama siber yang difasilitasi Interpol, penelitian ini menyusun tabel perbandingan tingkat partisipasi masing-masing negara. Tabel 2 membantu mengilustrasikan sejauh mana perbedaan kapasitas teknis, pemanfaatan platform intelijen, serta partisipasi dalam operasi dan pelatihan. Dari Tabel 2 terlihat jelas adanya kesenjangan signifikan dalam tingkat keterlibatan ASEAN. Negara dengan infrastruktur digital lebih maju seperti Singapura, Malaysia, dan Indonesia menunjukkan keterlibatan tinggi dalam operasi Interpol serta pemanfaatan platform I-24/7. Sebaliknya, negara seperti Laos, Kamboja, dan Myanmar masih berada pada tingkat rendah baik dari sisi kapasitas maupun partisipasi. Variasi ini memperkuat argumen bahwa strategi kolaborasi tidak dapat bersifat seragam, melainkan harus disesuaikan dengan kebutuhan spesifik tiap negara. Oleh karena itu, peran Interpol menjadi penting sebagai jembatan untuk mengurangi disparitas, agar beban penanggulangan kejahatan siber tidak timpang ("asymmetric burden") dan seluruh kawasan dapat merespons ancaman digital secara lebih merata dan efektif.

Tabel 2. Perbandingan Tingkat Keterlibatan Negara ASEAN dalam Kerja Sama Siber yang Difasilitasi Interpol (2019–2024)

Negara	Tingkat Keterlibatan dalam Operasi Interpol	Pemanfaatan I-24/7	Partisipasi Pelatihan Teknis	Tantangan Utama
Singapura	Sangat Tinggi (Night Fury, Haechi)	Optimal	Tinggi	Fragmentasi regulasi regional
Malaysia	Tinggi (Haechi)	Optimal	Tinggi	Kebutuhan koordinasi antarinstansi
Indonesia	Tinggi (Haechi, pelatihan teknis)	Sedang–Optimal	Tinggi	Infrastruktur digital belum merata
Filipina	Sedang (Haechi)	Sedang	Sedang	Kapasitas teknis terbatas
Thailand	Sedang (pelatihan teknis)	Sedang	Sedang	Koordinasi kelembagaan
Vietnam	Sedang (Night Fury)	Sedang	Sedang	Perbedaan regulasi domestik
Laos	Rendah	Terbatas	Rendah	Minimnya SDM & infrastruktur
Kamboja	Rendah	Terbatas	Rendah	Belum ada unit siber nasional
Myanmar	Rendah	Terbatas	Rendah	Instabilitas politik & prioritas rendah
Brunei	Rendah	Sedang	Rendah	Kapasitas forensik digital terbatas

B. Hasil Berdasarkan Tujuan Penelitian

Sesuai dengan tujuan utama penelitian, yakni untuk mengevaluasi peran Interpol dalam menangani kejahatan siber lintas negara di Asia Tenggara, hasil dianalisis berdasarkan tiga fokus utama: pertukaran intelijen, pelatihan teknis, dan operasi terkoordinasi antarnegara. Pertama, pada aspek pertukaran intelijen, Interpol telah menerapkan platform I-24/7 yang memfasilitasi pelaporan dan distribusi data kriminal siber antarnegara. Hampir seluruh negara ASEAN telah mengakses platform ini, namun efektivitasnya masih bergantung pada kesiapan infrastruktur dan komitmen tiap negara dalam berbagi informasi. Selain itu, masih ditemukan kesenjangan dalam kecepatan respons antarnegara saat terjadi insiden siber yang memerlukan tindakan cepat dan koordinasi lintas batas.

Kedua, dalam hal penguatan kapasitas sumber daya manusia, Interpol menyelenggarakan pelatihan digital forensik dan investigasi siber yang diikuti oleh aparat penegak hukum dari berbagai negara. Negara-negara seperti Indonesia, Thailand, Laos, dan Kamboja menunjukkan peningkatan partisipasi setiap tahun, menandakan adanya komitmen terhadap peningkatan kompetensi teknis dalam menghadapi kejahatan siber. Ketiga, pada aspek operasi terkoordinasi, kegiatan seperti Operation Haechi dan Night Fury mencerminkan keberhasilan Interpol dalam memfasilitasi aksi kolaboratif antarnegara. Operasi ini menargetkan pelaku kejahatan daring lintas batas, dan menghasilkan penangkapan pelaku serta penyitaan aset digital. Meski demikian, keterlibatan negara ASEAN dalam operasi tersebut masih belum merata karena kendala teknis dan logistik.

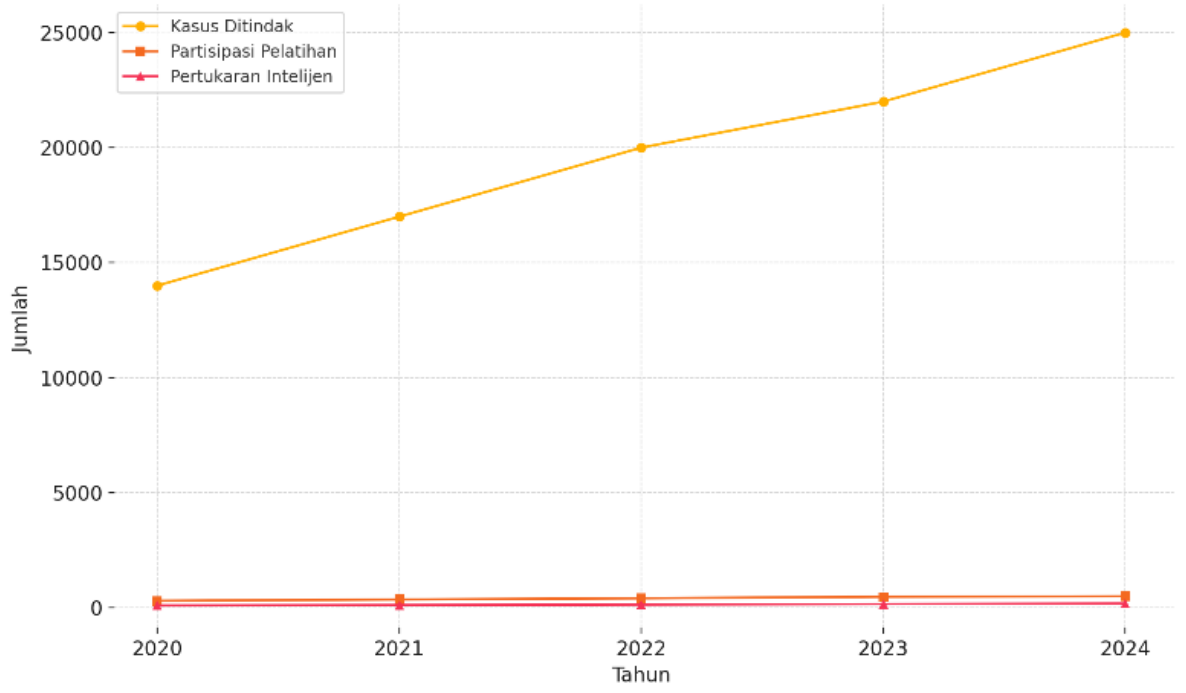
C. Hasil Uji Statistik atau Analisis Data

Meskipun pendekatan utama penelitian ini bersifat kualitatif, data kuantitatif digunakan untuk memperkuat penyajian hasil melalui analisis deskriptif. Statistik yang dihimpun meliputi jumlah kasus yang ditangani Interpol, tingkat partisipasi pelatihan, dan frekuensi pertukaran intelijen per bulan. Tabel 3 menyajikan data rata-rata dan ukuran penyebaran dari indikator utama yang diperoleh. Data ini membantu memberikan gambaran yang lebih rinci mengenai efektivitas kerja sama antarnegara dalam penanggulangan kejahatan transnasional.

Tabel 3. Statistik Deskriptif Indikator Kerja Sama Siber Regional ASEAN melalui Interpol (2020–2024)

Variabel	Rata-rata (2020–2024)	Standar Deviasi	Peningkatan Tahunan (%)
Kasus yang ditindak melalui Interpol	19.300 kasus/tahun	±4.500	18%
Partisipasi pelatihan	410 aparat/tahun	±85	25%
Frekuensi pertukaran intelijen	140 kasus/bulan	±30	21%

Data menunjukkan bahwa kerja sama regional yang difasilitasi Interpol mengalami perkembangan positif dari tahun ke tahun. Jumlah kasus yang ditindak meningkat 18% tiap tahun, mencerminkan efektivitas operasi lintas negara. Partisipasi pelatihan meningkat 25% per tahun, menunjukkan peningkatan kapasitas aparat penegak hukum. Pertukaran intelijen meningkat 21% per tahun, menandakan semakin aktifnya kolaborasi data antarnegara ASEAN. Gambaran tren kenaikan indikator-indikator tersebut selama periode 2020–2024 ditampilkan dalam Gambar 2.



Gambar 2. Tren Indikator Kerja Sama Siber Regional ASEAN melalui Interpol (2020–2024)

Gambar 2 menunjukkan tren peningkatan tahunan pada tiga indikator utama kerja sama siber: jumlah kasus yang ditindak melalui Interpol, partisipasi dalam pelatihan teknis, dan frekuensi pertukaran intelijen. Terlihat bahwa seluruh indikator mengalami pertumbuhan konsisten selama periode lima

tahun, yang mencerminkan efektivitas program dan peningkatan kolaborasi antarnegara ASEAN dalam menghadapi kejahatan siber lintas batas.

D. Hasil Utama yang Signifikan

Berdasarkan keseluruhan temuan dalam penelitian ini, terdapat sejumlah poin utama yang menunjukkan efektivitas serta tantangan dalam pelaksanaan kerja sama penanggulangan kejahatan siber di kawasan Asia Tenggara. Pertama, kolaborasi operasional yang dikoordinasikan oleh Interpol terbukti memberikan hasil nyata, khususnya dalam menangani kasus-kasus penipuan daring lintas negara dan serangan phishing, yang ditunjukkan melalui keberhasilan penangkapan pelaku dan penyitaan aset digital. Meskipun demikian, keterlibatan negara-negara anggota ASEAN dalam berbagai inisiatif ini masih belum merata. Ketimpangan tersebut sebagian besar dipengaruhi oleh perbedaan dalam kapasitas teknologi informasi, kesiapan kelembagaan, serta belum seragamnya regulasi nasional yang mengatur penegakan hukum siber.

Selanjutnya, meskipun platform pertukaran intelijen kriminal seperti I-24/7 telah digunakan secara aktif oleh mayoritas negara ASEAN, sistem ini masih menghadapi kendala dalam integrasi data secara waktu nyata, yang menghambat optimalisasi respons cepat terhadap insiden siber lintas batas. Di sisi lain, Interpol telah menyelenggarakan pelatihan teknis yang dinilai berdampak positif terhadap peningkatan kompetensi aparat penegak hukum lokal. Namun, jangkauan pelatihan ini masih perlu diperluas agar semua negara anggota dapat memperoleh manfaat secara seimbang dan berkelanjutan. Secara keseluruhan, hasil-hasil tersebut menekankan pentingnya pembentukan kerangka kebijakan regional yang terstruktur dan inklusif guna memperkuat sinergi antarnegara dan meningkatkan kapasitas kawasan dalam menghadapi ancaman siber yang terus berkembang.

Diskusi

Penelitian ini menunjukkan bahwa Interpol memainkan peran strategis dalam memperkuat kolaborasi antarnegara di Asia Tenggara dalam menghadapi kejahatan siber lintas negara. Mekanisme pertukaran intelijen melalui platform I-24/7, penyelenggaraan pelatihan teknis, serta operasi terkoordinasi seperti Operation Haechi dan Night Fury, memberikan kontribusi nyata dalam mengurangi dampak kejahatan siber lintas batas (Idris et al., 2024). Temuan ini membuktikan bahwa Interpol tidak hanya berfungsi sebagai fasilitator informasi, tetapi juga sebagai penggerak utama dalam membangun kapasitas dan kesiapsiagaan negara-negara ASEAN terhadap ancaman siber (Gillard et al., 2023). Meskipun demikian, efektivitas kolaborasi ini masih bersifat parsial dan belum merata di seluruh kawasan. Perbedaan kapasitas infrastruktur, sumber daya manusia, dan komitmen politik antarnegara menjadi faktor determinan yang mempengaruhi keberhasilan implementasi kolaborasi (Newman et al., 2023).

Hasil penelitian ini konsisten dengan temuan (Hakmeh, 2024) yang menegaskan bahwa kerja sama internasional adalah kunci dalam menangani kejahatan siber global. Sejalan dengan temuan (Pepe et al., 2024) dalam konteks Singapura, studi ini mendukung bukti bahwa negara-negara dengan infrastruktur

digital yang kuat menunjukkan tingkat kolaborasi ilmiah yang lebih tinggi. Penelitian (Hukom & Setiadi, 2025) menegaskan bahwa "peningkatan kapasitas forensik digital serta mekanisme kerja sama internasional dalam penanganan kasus kejahatan siber lintas negara" menjadi faktor utama dalam efektivitas penegakan hukum siber. Namun, penelitian ini menawarkan kontribusi yang lebih luas dengan menunjukkan bahwa ketimpangan kapasitas antarnegara ASEAN memerlukan peran lembaga seperti Interpol untuk menyelaraskan dan memperkuat kerja sama.

Tidak seperti penelitian sebelumnya yang banyak berfokus pada pendekatan hukum atau teknologi, penelitian ini menempatkan peran kelembagaan dan koordinatif Interpol sebagai pusat analisis (Gerspacher & Dupont, 2007). Jika dibandingkan dengan model kerja sama internasional di kawasan lain, terlihat perbedaan mencolok. Uni Eropa telah mengembangkan kerangka hukum komprehensif seperti European Cybercrime Centre (EC3) yang memastikan harmonisasi regulasi lintas negara. Di Amerika, kerja sama lebih menekankan pada mekanisme bilateral melalui FBI dan Department of Homeland Security. Sebaliknya, ASEAN masih menghadapi hambatan kelembagaan dan disparitas kapasitas. Perbandingan ini menegaskan bahwa upaya ASEAN bersama Interpol perlu mengadopsi praktik baik dari kawasan lain, namun tetap menyesuaikannya dengan realitas politik dan kelembagaan regional. Dengan demikian, penelitian ini memperkaya literatur dengan memperkenalkan pendekatan kelembagaan sebagai dimensi penting dalam pengelolaan keamanan siber lintas negara.

Salah satu temuan yang tidak terduga adalah rendahnya tingkat partisipasi beberapa negara ASEAN dalam operasi terkoordinasi dan pelatihan yang difasilitasi Interpol, meskipun tingkat ancaman siber di kawasan tersebut meningkat signifikan (Tseen et al., 2025). Negara-negara seperti Laos, Kamboja, dan Myanmar tercatat memiliki tingkat keterlibatan yang lebih rendah dibandingkan negara-negara seperti Singapura, Indonesia, dan Malaysia. Hal ini dapat dijelaskan oleh keterbatasan sumber daya manusia, infrastruktur digital, serta perbedaan prioritas kebijakan keamanan siber di masing-masing negara (Lee et al., 2024). Hingga 2024, Laos dan Kamboja masih belum memiliki unit siber nasional yang sepenuhnya terintegrasi dengan sistem I-24/7 maupun mekanisme pertukaran informasi siber ASEAN (termasuk ASEAN Cybercrime Operations Desk), sehingga hal ini memperlambat kemampuan mereka dalam bertukar data dan merespons serangan siber lintas batas secara cepat. Kondisi ini memperjelas bahwa keberhasilan kolaborasi regional tidak hanya bergantung pada keberadaan sistem global, tetapi juga pada kesiapan internal dan harmonisasi kebijakan di tingkat nasional.

Dari perspektif teoritis, penelitian ini memperkuat penerapan teori institusionalisme global (Koga, 2015) dengan menunjukkan bagaimana norma, aturan, dan praktik internasional diadopsi dan diadaptasi dalam konteks kawasan ASEAN. Selain itu, teori jaringan penegakan hukum transnasional (Wang, 2024) terbukti relevan dalam menjelaskan bagaimana interaksi dan pola kolaborasi antaraktor mempengaruhi efektivitas penanganan kejahatan siber. Kontribusi teoretis penelitian ini terletak pada integrasi kedua teori tersebut dalam menganalisis peran Interpol sebagai katalisator koordinasi keamanan siber lintas negara. Dari sisi praktis, penelitian ini memberikan rekomendasi strategis bagi Interpol dan negara-

negara ASEAN untuk membangun kerangka kebijakan yang lebih harmonis, meningkatkan alokasi sumber daya di negara-negara dengan kapasitas rendah, memperluas jangkauan pelatihan teknis agar keterampilan aparat penegak hukum lebih merata, serta mengembangkan sistem pertukaran data intelijen yang lebih terintegrasi dan real-time.

Selain faktor teknis, hambatan politik, birokrasi, dan perbedaan hukum antarnegara juga menjadi penghalang utama dalam memperkuat kerja sama penegakan hukum. Beberapa negara ASEAN masih menghadapi fragmentasi regulasi siber, keterbatasan koordinasi antarinstansi domestik, serta rendahnya prioritas politik terhadap isu keamanan digital. Hal ini menyebabkan proses integrasi hukum regional berjalan lambat dan seringkali tidak sinkron dengan inisiatif global yang difasilitasi Interpol. Dengan demikian, strategi penegakan hukum tidak hanya membutuhkan kerangka operasional, tetapi juga diplomasi hukum dan politik yang intensif untuk mengurangi disparitas implementasi di tingkat nasional. Implikasi praktis ini sangat penting agar negara-negara dengan kapasitas rendah tidak menjadi titik lemah dalam sistem keamanan digital regional yang terintegrasi.

Untuk memperkuat efektivitas kerja sama siber ASEAN bersama Interpol, diperlukan peta jalan kebijakan yang lebih konkret dan terarah. Pertama, harmonisasi regulasi siber ASEAN harus diprioritaskan melalui pembentukan kerangka hukum regional yang dapat mengurangi fragmentasi regulasi dan memudahkan adopsi standar internasional. Kedua, pendanaan regional untuk peningkatan kapasitas perlu diwujudkan, khususnya ditujukan bagi negara-negara dengan risiko tinggi namun kapasitas rendah seperti Laos, Kamboja, dan Myanmar, sehingga tidak terjadi kesenjangan keamanan yang dapat dimanfaatkan aktor jahat. Ketiga, pengembangan sistem pertukaran intelijen real-time yang terintegrasi antarnegara anggota ASEAN perlu diakselerasi untuk memastikan respons cepat terhadap ancaman siber lintas batas. Peta jalan ini dapat menjadi instrumen strategis dalam memastikan bahwa seluruh negara ASEAN memiliki tingkat kesiapan yang relatif seimbang, sekaligus memperkuat posisi ASEAN dalam ekosistem keamanan siber global.

Penelitian ini memiliki beberapa keterbatasan yang perlu diakui untuk menjaga transparansi dan objektivitas ilmiah. Pertama, penelitian ini sepenuhnya berbasis pada analisis dokumen sekunder tanpa pengumpulan data primer, sehingga interpretasi hasil sangat bergantung pada ketersediaan dan validitas dokumen (Moilanen et al., 2022). Kedua, ruang lingkup penelitian terbatas pada kawasan Asia Tenggara, sehingga generalisasi hasil ke kawasan lain harus dilakukan dengan kehati-hatian (Salih et al., 2023). Ketiga, tingkat transparansi pelaporan insiden siber di negara-negara ASEAN tidak seragam, sehingga kemungkinan ada bias dalam data yang digunakan (Al Amosh & Khatib, 2024). Analisis di (Kharisma et al., 2024) menunjukkan bahwa "keamanan data pribadi merupakan isu utama dalam perlindungan konsumen digital", terhambat oleh kompleksitas regulasi dan rendahnya enforcement di Indonesia. Keterbatasan ini penting disampaikan agar pembaca memahami konteks keterbatasan analisis yang dilakukan.

Berdasarkan keterbatasan yang diidentifikasi, penelitian mendatang disarankan untuk melakukan wawancara mendalam dengan aktor kunci seperti aparat penegak hukum, pejabat Interpol, dan pembuat kebijakan (Deflem, 2024). Selain itu, pendekatan kuantitatif berbasis survei juga direkomendasikan untuk mengukur persepsi dan efektivitas kerja sama antarnegara secara lebih sistematis (Zeller, 2024). Penelitian mendatang sebaiknya juga memperluas kajian ke kawasan lain seperti Eropa, Afrika, atau Amerika Latin untuk membandingkan model kerja sama yang berbeda (Fu et al., 2022). Aspek lain yang penting untuk dianalisis adalah dimensi privasi data dan kedaulatan digital sebagai faktor yang mempengaruhi partisipasi negara-negara dalam pertukaran intelijen (Samuele Fratini et al., 2024). Dengan pendekatan yang lebih holistik, interdisipliner, dan multi-metode, penelitian di masa depan diharapkan mampu memperluas pemahaman tentang kerja sama keamanan siber global secara lebih komprehensif.

IV. KESIMPULAN

Penelitian ini menegaskan bahwa Interpol memainkan peran penting dalam memperkuat kolaborasi antarnegara di Asia Tenggara dalam menghadapi kejahatan siber lintas negara. Melalui mekanisme pertukaran intelijen, pelatihan teknis, dan operasi terkoordinasi, Interpol telah memberikan kontribusi nyata dalam meningkatkan kapasitas penegakan hukum di kawasan ini. Temuan penelitian menunjukkan bahwa meskipun kerja sama yang difasilitasi Interpol menunjukkan tren positif, tantangan berupa ketimpangan kapasitas, perbedaan kebijakan, dan keterbatasan infrastruktur digital masih menghambat optimalisasi kolaborasi lintas negara.

Hasil penelitian ini berkontribusi secara teoritis dengan memperluas pemahaman mengenai peran organisasi internasional dalam keamanan siber regional, serta secara praktis memberikan rekomendasi strategis bagi penguatan kerja sama ASEAN di masa mendatang. Penelitian ini telah berhasil menjawab tujuan awal dengan menggambarkan secara komprehensif bagaimana Interpol memfasilitasi dan mengoordinasikan respons terhadap kejahatan siber di kawasan yang heterogen. Ke depan, penelitian lanjutan yang mengadopsi pendekatan empiris berbasis data primer serta memperluas konteks geografis akan memperkaya pemahaman dan mendukung terwujudnya ekosistem keamanan siber global yang lebih inklusif dan adaptif.

REFERENSI

Al Amosh, H., & Khatib, S. F. A. (2024). Cybersecurity Transparency and Firm Success: Insights From the Australian Landscape. *Australian Economic Papers*, *64*(2), 189–204. https://doi.org/10.1111/1467-8454.12385

Ali, A., Shah, M., Foster, M., & Alraja, M. N. (2025). Cybercrime Resilience in the Era of Advanced Technologies: Evidence from the Financial Sector of a Developing Country. *Computers*, *14*(2), 38. https://doi.org/10.3390/computers14020038

Bekkers, L., Leukfeldt, R., & Kleemans, E. (2025). Police Investigations Into Financial-Economic Cybercriminal Networks: The Experiences and Perceptions of Dutch Law Enforcement. *European Journal on Criminal Policy and Research*, *0123456789*. https://doi.org/10.1007/s10610-025-

09615-2

Cieslik, A., & Ghodsi, M. (2024). The Impact of Regulatory Divergence in Non-Tariff Measures on the Cross-Border Investment of Multinationals. *Emerging Markets Finance and Trade*, *60*(15), 3598–3637. https://doi.org/10.1080/1540496x.2024.2356870

Deflem, M. (2024). The Declining Significance of Interpol: Policing International Terrorism After 9/11. *International Criminal Justice Review*, *34*(1), 5–19. https://doi.org/10.1177/10575677221136175

Farber, S. (2025). The Evolving Nexus of Cybercrime and Terrorism: A Systematic Review of Convergence and Policy Implications. *Security Journal*, *38*(1), 1–23. https://doi.org/10.1057/s41284-025-00471-7

Ferdinan Sitompul, Manik, A. P. P., Sinaga, C. D., Purba, A. T., & Satria, A. (2024). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Hukum Indonesia. *Jaksa : Jurnal Kajian Ilmu Hukum Dan Politik*, *2*(2), 222–228. https://doi.org/10.51903/jaksa.v2i2.1668

Fu, Y. C., Marques, M., Tseng, Y. H., Powell, J. J. W., & Baker, D. P. (2022). An Evolving International Research Collaboration Network: Spatial and Thematic Developments in Co-Authored Higher Education Research. *Scientometrics*, *127*(3), 1403–1429. https://doi.org/10.1007/s11192-021-04200-w

Gerspacher, N., & Dupont, B. (2007). The Nodal Structure of International Police Cooperation: An Exploration of Transnational Security Networks. *Global Governance*, *13*(3), 347–364. https://doi.org/10.1163/19426720-01303005

Gillard, S., David, D. P., Mermoud, A., & Maillart, T. (2023). Efficient Collective Action for Tackling Time-Critical Cybersecurity Threats. *Journal of Cybersecurity*, *9*(1), 0–22. https://doi.org/10.1093/cybsec/tyad021

Hakmeh, J. (2024). The UN Convention on Cybercrime: A Milestone in Cybercrime Cooperation? *Journal of Cyber Policy*, *9*(2), 125–130. https://doi.org/10.1080/23738871.2024.2441549

Hongyue Jin, & Guo, X. (2023). Annual Report 2023. *Clean Technologies and Recycling*, *3*(4), 302–306. https://doi.org/10.3934/ctr.2023020

Hukom, R., & Setiadi, M. H. (2025). Pengaruh Media Sosial terhadap Pola Kejahatan di Era Digital: Studi Kriminologi dengan Pendekatan Netnografi. *Perkara : Jurnal Ilmu Hukum Dan Politik*, *3*(1), 750–768. https://doi.org/10.51903/perkara.v3i1.2353

Idris, M. F., Laksito, J., & Ariyani, W. (2024). Tanggung Jawab Hukum Perusahaan Teknologi Atas Penyalahgunaan Data Pengguna: Studi Kasus Di ASEAN. *Jaksa : Jurnal Kajian Ilmu Hukum Dan Politik*, *2*(4), 45–46. https://doi.org/10.51903/jaksa.v2i4.2268

Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore †. *Laws*, *13*(4), 1–19. https://doi.org/10.3390/laws13040044

Kharisma, D., Susanti, E., Aprili, R., Info, A., Transactions, D., & Protection, C. (2024). Evaluasi Kebijakan Perlindungan Konsumen dalam Transaksi Digital di Indonesia: Studi Kebijakan dan Analisis SWOT. *Perkara: Jurnal Ilmu Hukum Dan Politik*, *2*(4), 565–578. https://doi.org/10.51903/perkara.v2i4.2228

Koga, K. (2015). ASEAN , Institutional Change , and Historical Institutionalism. *E-International*

Relations, 8–11. https://www.e-ir.info/2015/10/31/asean-institutional-change-and-historical-institutionalism/

Laksito, J., Idris, M. F., & Waryanto, A. (2024). Hak dan Kewajiban Negara dalam Mengatasi Kejahatan Lintas Batas di Era Digital: Pendekatan Analisis Normatif. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *2*(4), 774–790. https://doi.org/10.51903/hakim.v2i4.2154

Lazarus, S., Chiang, M., & Button, M. (2025). Assessing Human Trafficking and Cybercrime Intersections Through Survivor Narratives. *Deviant Behavior*, *37*(4), 1–27. https://doi.org/10.1080/01639625.2025.2470402

Lee, G. S., Kim, S. H., Lee, I. Y., Brown, S., & Carbajal, Y. A. (2024). Adapting Cybersecurity Maturity Models for Resource-Constrained Settings: A Case Study of Peru. *Electronic Journal of Information Systems in Developing Countries*, *91*(1), 12350. https://doi.org/10.1002/isd2.12350

Ma, M., Yang, Z., Li, L., & Lam, F. I. (2024). How is Regional Cooperation Possible in Cross-Border Institutional Conflicts? The Guangdong-Hong Kong-Macao Cooperation from the Perspective of the Sociology of Knowledge. *Journal of Infrastructure, Policy and Development*, *8*(9), 7178. https://doi.org/10.24294/jipd.v8i9.7178

Marjun, Saroji, & Farhan, F. (2025). Cyberbullying and Legal Protection for Victims in the Digital Era: A Case Study on Social Media Platforms. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *3*(1), 955–973. https://doi.org/10.51903/hakim.v3i1.2290

Moilanen, T., Sivonen, M., Hipp, K., Kallio, H., Papinaho, O., Stolt, M., Turjamaa, R., Häggman-Laitila, A., & Kangasniemi, M. (2022). Developing a Feasible and Credible Method for Analyzing Healthcare Documents as Written Data. *Global Qualitative Nursing Research*, *9*, 1–13. https://doi.org/10.1177/23333936221108706

Newman, A., Ferrer, J., Andresen, M., & Zhang, Y. (2023). Human Resource Management in Times of Crisis: What Have We Learnt from the Recent Pandemic? *International Journal of Human Resource Management*, *34*(15), 2857–2875. https://doi.org/10.1080/09585192.2023.2229100

Pepe, C. G. E., Fonseca, M. V. A., & Silva Marques, C. F. (2024). International Collaboration Towards Innovation Management: A Network Perspective and the Global Innovation Index. *Journal of Innovation and Entrepreneurship*, *13*(1), 32. https://doi.org/10.1186/s13731-024-00384-6

Sachoulidou, A. (2024). Cross-Border Access to Electronic Evidence in Criminal Matters: The New EU Legislation and the Consolidation of a Paradigm Shift in the Area of 'Judicial' Cooperation. *New Journal of European Criminal Law*, *15*(3), 256–274. https://doi.org/10.1177/20322844241258649

Salih, S., Hamid, T. A., Ibrahim, R., Ashari, A., Abdullah, S. F., & Tyng, C. Sen. (2023). A Scoping Review on Determinants of Active Ageing in Southeast Asian Region. *Sains Malaysiana*, *52*(5), 1523–1543. https://doi.org/10.17576/jsm-2023-5205-15

Samuele Fratini et al. (2024). Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *Digital Society*, *3*(3), 59. https://doi.org/10.2139/ssrn.4816020

Scholte, J. A. (2021). Beyond Institutionalism: Toward a Transformed Global Governance Theory. *International Theory*, *13*(1), 179–191. https://doi.org/10.1017/S1752971920000421

Sundram, P. (2024). ASEAN Cooperation to Combat Transnational Crime: Progress, Perils, and

Prospects. *Frontiers in Political Science*, *6*, 1304828. https://doi.org/10.3389/fpos.2024.1304828

Tseen, B., Lee, F., Kornphetcharat, K., & Sims, J. P. (2025). ASEAN Cybersecurity Cooperation Strategy : Combating Cyber Terrorism and Hackers Through CERT Coordination ASEAN Cybersecurity Cooperation Strategy : *International Journal of Law and Public Policy (IJLAPP)*, *7*(1), 20–30. https://doi.org/10.36079/lamintang.ijlapp-0701.788

Wang, X. (2024). Global (Re-)Framing of Cybercrime: An Emerging Common Interest in Flux of Competing Normative Powers? *Leiden Journal of International Law*, 1–27. https://doi.org/10.1017/s0922156524000402

Wilner et al. (2024). Offensive Cyber Operations and State Power: Lessons from Russia in Ukraine. *International Journal*, *79*(1), 138–148. https://doi.org/10.1177/00207020241234228

Zeller, A. (2024). Measuring Democratic Legitimacy within Regional Organizations - A Member States' Perspective. *Frontiers in Political Science*, *6*, 109–111. https://doi.org/10.3389/fpos.2024.1359645

Zhou, Y., Tiwari, M., Bernot, A., & Lin, K. (2024). Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality. *Asian Journal of Criminology*, *19*(3), 419–439. https://doi.org/10.1007/s11417-024-09436-y