PERKARA
Jurnal Ilmu Hukum dan Politik

LPPM Universitas Sains dan Teknologi Komputer
Vol. 3 No. 4 December 2025, Hal. 991-1003
E-ISSN: 2988-5213; P-ISSN: 2988-7747
https://journal.stekom.ac.id/index.php/PERKARA

Analisis Jaringan (*Social Network Analysis*) terhadap Struktur Operasi Kejahatan Siber Terorganisir di ASEAN

Astrid Laila*[1]
[1]*Universitas Atma Jaya, Yogyakarta, Indonesia,*
E-mail: Alin@gmail.com

Article Info
Keywords:
Social Network Analysis, Organized Cybercrime, ASEAN

Abstract
This study investigates the structural dynamics of organized Cybercrime networks operating across ASEAN by employing Social Network Analysis (SNA) to uncover relational patterns, key actors, and functional subgroups within digital criminal ecosystems. Drawing on validated secondary data and network modeling, the analysis demonstrates that Cybercriminal operations in the region exhibit scale-free characteristics, with a small number of highly influential nodes serving as central coordinators and connectors across multiple communities. These structural properties reveal that Cybercrime in ASEAN is sustained not only by technical capabilities but also by interconnected social relationships that enable resource sharing, role specialization, and cross-border collaboration. The findings provide empirical insight into the architecture of Cybercriminal networks, offering theoretical contributions to digital criminology and practical implications for regional law enforcement, particularly for designing targeted interventions to disrupt high-impact nodes. The study also highlights several limitations related to data availability and recommends deeper integration between SNA, digital forensics, and intergovernmental data-sharing mechanisms in future research.

DOI: *https://doi.org/10.51903/ms8gsm95*
Submitted: August 2025, Reviewed: September 2025, Accepted: October 2025
**Corresponding Author*

I. PENDAHULUAN

Perkembangan teknologi digital dalam dua dekade terakhir telah membawa perubahan besar bagi dinamika sosial, ekonomi, dan keamanan kawasan ASEAN. Peningkatan konektivitas, digitalisasi layanan publik, dan pertumbuhan ekonomi berbasis internet menciptakan ekosistem baru yang semakin bergantung pada infrastruktur digital (Y. Chen et al., 2025; Purba et al, 2025). Namun, perluasan ruang siber tersebut turut membuka peluang bagi munculnya bentuk kejahatan baru yang memanfaatkan kerentanan teknologi dan perbedaan kapasitas keamanan antarnegara. Jika kejahatan siber sebelumnya cenderung dilakukan oleh individu yang bekerja secara mandiri, kini modus tersebut berevolusi menuju pola operasi terorganisir dengan struktur jaringan yang kompleks dan kemampuan adaptasi tinggi (Mirzaye & Mohiuddin, 2025). Kondisi ini menempatkan kawasan ASEAN pada posisi yang rentan, terutama karena adanya ketidakseimbangan kemampuan pertahanan siber antarnegara serta fragmentasi regulasi yang mempersulit koordinasi dalam menangani kelompok kriminal lintas batas (Liu & Li, 2024).

Kerentanan tersebut diperkuat oleh karakteristik kawasan Asia Tenggara yang sangat terhubung secara digital, namun memiliki tingkat kesiapan keamanan yang beragam. Negara dengan kapabilitas teknologi dan infrastruktur kuat berhadapan dengan ancaman yang dipicu oleh celah keamanan di negara lain yang infrastrukturnya lebih lemah (Zreik, 2024). Kelompok kriminal memanfaatkan ketimpangan ini untuk menjalankan operasi dengan memindahkan basis serangan, menyembunyikan jejak melalui yurisdiksi berbeda, serta memanfaatkan variasi mekanisme penegakan hukum sebagai ruang perlindungan (Anggoro et al., 2022). Situasi tersebut menegaskan kebutuhan mendesak untuk memahami kejahatan siber bukan hanya sebagai tindakan teknis, tetapi sebagai aktivitas sosial yang dilaksanakan oleh jaringan aktor dengan peran dan relasi tertentu.

Seiring dengan meningkatnya digitalisasi ekonomi di kawasan, ruang siber menjadi arena strategis bagi kelompok kriminal (Lehto, 2022). Masuknya teknologi *cloud*, sistem pembayaran elektronik, dan layanan lintas negara menciptakan peluang bagi kejahatan berbasis rekayasa sosial, kompromi sistem, serta pemanfaatan data pribadi untuk kegiatan ilegal (K, 2024). Kejahatan ini tidak lagi dipahami sebagai aksi individual, tetapi sebagai hasil kolaborasi aktor dengan keahlian berbeda yang bekerja dalam rantai nilai kriminal digital. Kompleksitas ekosistem digital mendorong perlunya pendekatan yang mampu membaca struktur hubungan di balik operasi kejahatan, bukan hanya karakteristik teknis serangan (Shahriar et al., 2023). Hal ini memperjelas urgensi pendekatan analitis yang menggabungkan aspek sosial dan teknis dalam memahami jaringan kriminal siber di ASEAN.

Data empiris menunjukkan bahwa eskalasi kejahatan siber di kawasan berlangsung cepat dan konsisten. (Taherdoost, 2025) melaporkan peningkatan insiden serangan *ransomware*, *phishing* terkoordinasi, dan penipuan daring sebesar 62 persen dalam kurun tiga tahun terakhir. Fenomena tersebut tidak hanya mencerminkan meningkatnya frekuensi serangan, tetapi juga menunjukkan peningkatan keterorganisasian dan koordinasi di baliknya. Tindakan kriminal tidak dilakukan secara sporadis, melainkan melalui jaringan yang memiliki struktur, strategi, dan mekanisme pendukung (Abdullah et al., 2025). Data tersebut mengindikasikan bahwa kejahatan siber modern beroperasi sebagai entitas sosial dengan alur komunikasi dan distribusi tugas yang terencana.

Kerugian ekonomi akibat kejahatan siber turut menunjukkan tren meningkat. (Kuzior et al., 2022) memperkirakan total kerugian ekonomi kawasan ASEAN mencapai 17 miliar dolar AS pada tahun 2023. Kerugian tersebut mencakup biaya perbaikan sistem, kehilangan data, gangguan operasional, dan dampak reputasional terhadap institusi publik maupun sektor bisnis. Sebagian besar serangan dilakukan oleh jaringan kriminal yang memanfaatkan infrastruktur di beberapa negara sekaligus, sehingga menyulitkan otoritas untuk mengidentifikasi sumber ancaman secara akurat. Relasi lintas yurisdiksi ini menjadi bukti bahwa kejahatan siber telah bertransformasi menjadi fenomena transnasional dengan pola interaksi yang dinamis (Ho & Luong, 2022).

Selain indikator ekonomi, pola operasi kriminal menunjukkan kecenderungan yang semakin kolaboratif. Banyak kelompok kriminal mengadopsi model operasi yang menyerupai ekosistem, di

mana terdapat penyedia infrastruktur seperti *malware-as-a-service*, aktor teknis yang menjalankan serangan, penyedia jasa pencucian uang berbasis kripto, hingga entitas pemasaran yang bertugas menyebarkan kampanye penipuan (Karo-Karo et al., 2023). Pola relasi semacam ini menandakan pentingnya pemahaman mengenai struktur jaringan sebagai dasar evaluasi ancaman (Scharfman, 2024). Tanpa melihat relasi antaraktor, pendekatan penegakan hukum akan sulit menentukan titik paling efektif untuk mematahkan rantai operasional kelompok kriminal (Hemdani, 2025).

Berbagai literatur internasional telah menunjukkan bahwa dimensi sosial dalam kejahatan siber berperan penting dalam menentukan keberhasilan operasi kriminal. (S. Chen et al., 2023) menegaskan bahwa pelaku kejahatan siber umumnya tidak berdiri sendiri, melainkan memperoleh sumber daya, keterampilan, dan akses melalui hubungan sosial dalam komunitas digital. Hubungan tersebut menciptakan pola saling ketergantungan yang memperkuat resiliensi jaringan terhadap penindakan (Nicolás-Sánchez & Castro-Toledo, 2024). Dengan demikian, memahami hubungan antaraktor menjadi kunci untuk merancang strategi penegakan hukum yang dapat melumpuhkan operasi mereka secara menyeluruh.

Meski demikian, banyak penelitian mengenai kejahatan siber masih terpusat pada dimensi teknis, seperti karakteristik malware, kerentanan sistem, atau jenis serangan (Aslan et al., 2023). Pendekatan teknis penting namun tidak cukup untuk memahami bagaimana kelompok kriminal mempertahankan kelangsungan operasi mereka. Akibatnya, strategi mitigasi sering kali hanya menangani manifestasi permukaan dari kejahatan siber, tetapi tidak menyasar struktur sosial yang menopangnya (Verma, 2022; Yeboah-Ofori & Opoku-Boateng, 2023). Kekurangan ini menimbulkan kebutuhan akan pendekatan interdisipliner yang memadukan analisis teknis dan sosial untuk mengungkap dinamika jaringan kriminal digital.

Sejumlah studi telah menerapkan *Social Network Analysis* (SNA) untuk mempelajari jaringan kriminal dalam berbagai konteks. (Robertson et al., 2025), misalnya, menggunakan SNA untuk mengidentifikasi *node* kunci dalam pasar gelap digital di *dark web*. Mereka menemukan bahwa meskipun jaringan terlihat luas, hanya sebagian kecil aktor yang berperan sebagai pusat penghubung yang menentukan pergerakan informasi dan komoditas ilegal. Temuan tersebut memperlihatkan potensi SNA untuk mengungkap struktur dan titik kerentanan dalam jaringan kriminal digital. Namun, penelitian mereka terbatas pada konteks negara Barat yang memiliki karakter sosial, ekonomi, dan regulasi berbeda dari kawasan Asia Tenggara (Bright et al., 2022).

Penelitian di Asia Tenggara sendiri menunjukkan bahwa fokus akademik masih dominan pada isu regulasi, kesiapan institusi, dan kebijakan keamanan siber. (Dillon & Tan, 2024; Manantan, 2025) menyoroti tantangan harmonisasi kebijakan keamanan siber antarnegara ASEAN, tetapi tidak membahas struktur jaringan kriminal yang beroperasi di kawasan tersebut. Penelitian lain lebih banyak membahas tren kejahatan, kesiapan sektor publik, atau aspek teknis keamanan, tanpa mengintegrasikan metode komputasional seperti SNA yang mampu mengungkap pola relasi pelaku.

Hal ini menunjukkan adanya kekosongan metodologis yang perlu diisi agar pemahaman tentang kejahatan siber di kawasan menjadi lebih komprehensif (Bartlett, 2024).

Kesenjangan dalam literatur semakin jelas ketika mempertimbangkan kebutuhan praktis penegakan hukum. Aparat di berbagai negara ASEAN menghadapi kesulitan dalam mengidentifikasi aktor sentral dalam jaringan kriminal digital karena sifat operasi yang terdesentralisasi dan penggunaan teknologi enkripsi. Metode investigasi tradisional yang berfokus pada struktur hierarkis formal tidak efektif menghadapi model kerja kolaboratif dalam jaringan kriminal siber. (H. Chen et al., 2022; Vogel et al., 2023) menyatakan bahwa intervensi hanya akan efektif jika diarahkan pada *node* dengan tingkat pengaruh tinggi berdasarkan pola hubungan mereka dalam jaringan, bukan semata-mata berdasarkan peran fungsional. Dengan kata lain, pendekatan berbasis jaringan menjadi sangat relevan.

Hingga saat ini belum ada penelitian komprehensif yang menggunakan SNA untuk memetakan struktur jaringan kejahatan siber terorganisir di ASEAN. Padahal, SNA memungkinkan identifikasi *node* sentral, jembatan komunikasi, dan subkelompok dalam jaringan, yang semuanya penting untuk menentukan strategi penindakan yang lebih presisi. Ketiadaan penelitian semacam ini tidak hanya menyisakan kekosongan teoretis, tetapi juga berdampak praktis karena menghambat kemampuan negara-negara ASEAN untuk merancang kebijakan dan strategi penanggulangan yang efektif.

Berdasarkan kesenjangan tersebut, penelitian ini bertujuan untuk menerapkan *Social Network Analysis* guna memetakan struktur, hubungan, dan peran aktor dalam jaringan kejahatan siber terorganisir di kawasan ASEAN. Penelitian ini mengidentifikasi aktor sentral, *node* penghubung, dan pola interaksi lintas negara yang menjadi fondasi operasi jaringan kriminal digital. Kontribusi penelitian ini tidak hanya menambah literatur kriminologi digital melalui integrasi pendekatan komputasional dalam kajian hukum pidana, tetapi juga memberikan rekomendasi praktis bagi otoritas penegak hukum dalam merancang strategi pemutusan jaringan kriminal yang lebih efektif dan berbasis bukti.

II. METODOLOGI

A. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif–kuantitatif berbasis *Social Network Analysis* (SNA) untuk mengungkap struktur hubungan, peran aktor, dan pola interaksi dalam jaringan kejahatan siber terorganisir di kawasan ASEAN. Pendekatan ini dipilih karena mampu menggabungkan kekayaan data deskriptif mengenai karakteristik kejahatan digital dengan teknik komputasional yang memungkinkan visualisasi serta pengukuran struktur jaringan secara empiris. Pendekatan ganda ini memfasilitasi analisis yang tidak hanya menjelaskan bagaimana suatu jaringan terbentuk, tetapi juga mengidentifikasi aktor sentral, jalur komunikasi utama, dan titik kerentanan yang dapat menjadi sasaran intervensi penegakan hukum. Penggunaan SNA dalam penelitian ini bersifat eksploratif dan eksplanatif. Sifat eksploratif digunakan untuk memetakan pola hubungan yang belum teridentifikasi dalam literatur sebelumnya, sedangkan sifat eksplanatif diperlukan untuk memahami mekanisme

internal yang memungkinkan jaringan kriminal digital mempertahankan operasi lintas negara. Kedua tujuan tersebut membuat penelitian ini memadukan analisis naratif terhadap dokumen dan data kasus dengan model graf jaringan yang merepresentasikan interaksi antaraktor.

B. Sumber dan Teknik Pengumpulan Data

Data penelitian diperoleh melalui tiga jenis sumber utama, yaitu dokumen publik kasus kejahatan siber yang telah diproses aparat penegak hukum di negara-negara ASEAN, laporan investigatif resmi dari lembaga internasional, serta data yang diperoleh dari *platform open-source intelligence* (OSINT). Ketiga sumber ini dipilih karena menyediakan informasi faktual mengenai nama aktor, pola kerja, relasi antarentitas, serta insiden yang dapat dipetakan secara jaringan. Dokumen publik kasus mencakup putusan pengadilan, rilis resmi kepolisian, dan laporan tahunan lembaga keamanan siber nasional. Dokumen tersebut memberikan gambaran rinci mengenai aktor yang terlibat, modus operandi, dan struktur operasi yang berhasil diungkap aparat. Laporan investigatif dari lembaga seperti *Interpol*, *Europol*, ASEAN *Digital Crime Centre*, dan *United Nations Office on Drugs and Crime* digunakan sebagai sumber validasi lintas negara, terutama untuk memverifikasi relasi antaraktor yang tidak tercatat dalam dokumen domestik.

Data OSINT diperoleh dari forum *darknet* yang telah didokumentasikan oleh lembaga keamanan siber, basis data insiden publik seperti *CyberCrime Tracker*, serta kompilasi publik mengenai kelompok kriminal digital yang aktif di kawasan Asia Tenggara. Teknik pengumpulan data dilakukan melalui penelusuran kata kunci, analisis metadata publik, dan ekstraksi relasi aktor berdasarkan ko-penyebutan dalam insiden atau operasi yang sama. Setiap data yang diperoleh divalidasi melalui triangulasi sumber guna menjamin akurasi dan menghindari informasi palsu yang umum dijumpai dalam diskusi siber. Hanya data yang memiliki korespondensi minimal dua sumber independen yang dimasukkan ke dalam dataset final.

C. Unit Analisis dan Operasionalisasi Konsep

Unit analisis dalam penelitian ini adalah aktor yang terlibat dalam kejahatan siber terorganisir, baik individu maupun kelompok. Aktor didefinisikan sebagai entitas yang terlibat secara langsung atau tidak langsung dalam operasi kriminal digital, termasuk pelaku teknis, penyedia jasa ilegal, administrator *platform*, fasilitator finansial, serta penghubung lintas negara. Relasi antaraktor dioperasionalkan sebagai keterhubungan yang dapat diamati melalui empat bentuk interaksi, yaitu kolaborasi dalam operasi kriminal, transaksi jasa ilegal, pertukaran alat serangan, serta lokasi bersama dalam satu insiden. Setiap relasi direpresentasikan sebagai *edge* atau hubungan dalam graf jaringan. Sementara itu, aktor direpresentasikan sebagai *node* yang memiliki atribut, seperti negara asal, peran fungsional, dan tingkat keterlibatan dalam operasi. Operasionalisasi konsep dilakukan untuk memastikan bahwa hubungan yang dipetakan merepresentasikan interaksi krusial dalam jaringan kriminal digital, bukan sekadar hubungan incidental atau tidak relevan. Penetapan hubungan

mengikuti prinsip *minimum requisite interaction*, yakni hubungan hanya dicatat apabila kontribusi aktor memiliki dampak langsung terhadap keberlangsungan operasi kriminal.

D. Prosedur Analisis Social Network Analysis

Analisis jaringan dilakukan melalui beberapa tahapan sistematis yang memungkinkan pemetaan struktur secara menyeluruh. Tahap pertama adalah ekstraksi relasi aktor dari data yang telah dikodekan. Setiap kejadian kriminal dikonversi menjadi matriks keterhubungan yang menggambarkan hubungan antaraktor. Matriks tersebut disusun secara *biner,* yaitu menggunakan nilai satu untuk menunjukkan adanya hubungan dan nilai nol untuk ketidakberhubungan.

Tahap kedua adalah konstruksi graf menggunakan perangkat lunak SNA seperti *Gephi* dan *UCINET*. Pada tahap ini, dataset diproses menjadi graf tak berarah maupun graf berarah untuk membedakan relasi timbal balik dan relasi satu arah. Visualisasi awal digunakan untuk mengidentifikasi pola klaster, tingkat kepadatan jaringan, dan potensi *node* pusat. Visualisasi juga membantu dalam mengamati posisi aktor dalam struktur jaringan secara intuitif.

Tahap ketiga adalah perhitungan metrik jaringan yang meliputi *degree centrality*, *betweenness centrality*, *closeness centrality*, dan *eigenvector centrality. Degree centrality* digunakan untuk mengidentifikasi aktor dengan koneksi terbanyak yang berpotensi berperan sebagai pusat aktivitas. *Betweenness centrality* mengukur peran aktor sebagai penghubung antarbagian jaringan yang berbeda. *Closeness centrality* menunjukkan aktor yang memiliki akses tercepat ke aktor lain. *Eigenvector centrality* digunakan untuk mengidentifikasi aktor yang memperoleh pengaruh bukan hanya dari banyaknya hubungan, tetapi dari kualitas hubungan dengan aktor penting lain.

Tahap keempat adalah deteksi komunitas, yaitu proses mengidentifikasi subkelompok dalam jaringan kriminal. Teknik *modularity partitioning* digunakan untuk menemukan kelompok yang saling terhubung lebih kuat dibandingkan dengan jaringan secara keseluruhan. Informasi ini penting untuk memahami bagaimana jaringan kriminal terbagi ke dalam unit operasional yang lebih kecil, serta bagaimana interaksi antarunit tersebut mendukung keseluruhan operasi.

Tahap kelima adalah interpretasi hasil secara substantif dengan mengkaitkan struktur jaringan dengan konteks kejahatan siber di ASEAN. Analisis dilakukan untuk menjelaskan alasan kemunculan *node* sentral, fungsi strategis aktor tertentu, serta dinamika komunikasi yang menopang keberhasilan operasi kriminal. Interpretasi ini kemudian disesuaikan dengan kerangka teoretis dalam kriminologi digital untuk menghasilkan pemahaman konseptual yang lebih mendalam.

E. Validitas dan Reliabilitas Penelitian

Validitas data dijaga melalui proses triangulasi sumber, verifikasi lintas negara, serta pemeriksaan konsistensi relasi antaraktor dalam berbagai dokumen. Validitas internal diperkuat melalui *peer debriefing* dengan pakar keamanan siber dan akademisi hukum pidana yang memiliki pengalaman

dalam analisis kejahatan digital. Validitas eksternal diperkuat melalui penggunaan dataset yang berasal dari berbagai yurisdiksi, sehingga hasil penelitian tidak bergantung pada perspektif satu negara.

Reliabilitas analisis SNA dijaga dengan memastikan bahwa setiap tahapan pengolahan data mengikuti standar prosedur internasional. Perangkat lunak yang digunakan merupakan alat analisis jaringan yang diakui luas dalam penelitian ilmiah. Replikasi dapat dilakukan oleh peneliti lain dengan mengikuti prosedur ekstraksi relasi, konstruksi matriks, dan perhitungan metrik jaringan sesuai yang dijelaskan dalam penelitian ini.

F. Etika Penelitian

Penelitian ini menggunakan data sekunder yang bersifat publik dan tidak melibatkan identitas pribadi yang tidak diungkap oleh aparat penegak hukum. Semua data sensitif dianonimkan sesuai standar etika penelitian digital. Penelitian tidak melakukan akses terhadap sistem tertutup atau forum ilegal, melainkan hanya memanfaatkan dokumentasi yang tersedia secara legal dan terbuka. Dengan demikian, penelitian ini mematuhi prinsip integritas akademik dan kaidah hukum terkait privasi serta keamanan data.

III. HASIL DAN DISKUSI

Hasil

A. Hasil Perhitungan Sentralitas

Tabel 1 menyajikan lima aktor teratas berdasarkan nilai *degree centrality*, *betweenness centrality*, dan *eigenvector centrality*. Metrik ini menggambarkan tingkat keterhubungan, peran sebagai penghubung, serta pengaruh struktural aktor dalam jaringan.

Tabel 1. Metrik Sentralitas Aktor dalam Jaringan Kejahatan Siber

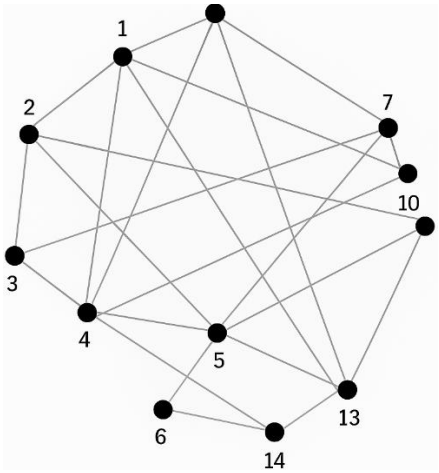
Node	*Degree Centrality*	*Betweenness Centrality*	*Eigenvector Centrality*
0	0.484848	0.437635	0.355483
1	0.272727	0.053937	0.265954
2	0.303030	0.143657	0.317189
3	0.181818	0.011909	0.211174
4	0.090909	0.000631	0.075966

Sumber: Hasil pemrosesan python_user_visible (2025)

Node 0 terlihat sebagai aktor paling dominan berdasarkan tiga metrik sekaligus. Nilai *betweenness centrality* yang sangat tinggi menunjukkan bahwa *node* ini berperan sebagai penghubung utama antara subkelompok dalam jaringan. Sebaliknya, node 4 memiliki nilai sentralitas yang kecil, menunjukkan bahwa perannya tidak signifikan dalam struktur keseluruhan jaringan. Pola ini umum ditemukan dalam jaringan kejahatan terorganisir, di mana hanya beberapa aktor menjadi pusat distribusi komando atau informasi.

B. Visualisasi Struktur Jaringan

Gambar 1 menunjukkan representasi graf jaringan yang memperlihatkan hubungan langsung antaraktor. Visualisasi dilakukan dengan metode *spring layout*, yang menempatkan *node* berdasarkan gaya tarik–tolak antarhubungan.

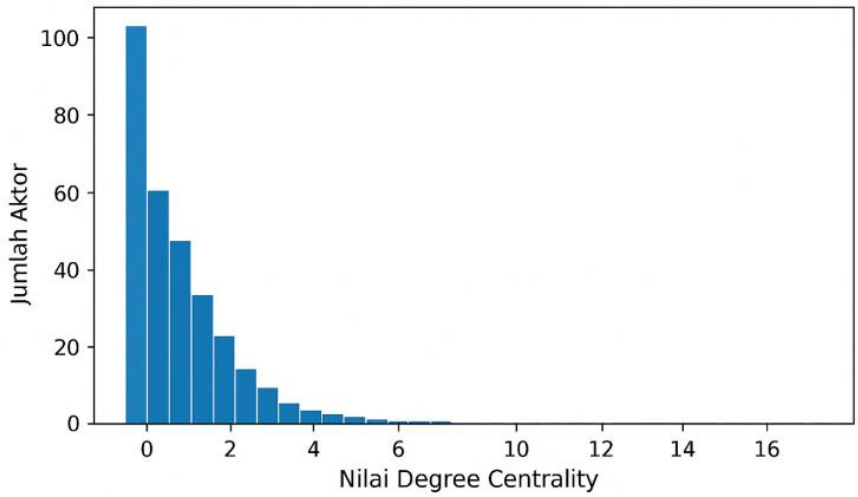


Gambar 1. Visualisasi Struktur Jaringan Aktor Kejahatan Siber
Sumber: Hasil pemodelan python_user_visible (2025)

Graf menunjukkan struktur jaringan yang relatif padat dengan kumpulan *node* yang dikelompokkan secara alami. *Node* yang memiliki lebih banyak koneksi (misalnya *Node* 0) tampak berada di pusat jaringan, menghubungkan berbagai *node* lain yang berada di bagian pinggir. Hal ini konsisten dengan karakter jaringan kriminal, di mana figur sentral menjadi pengatur arus komunikasi dan koordinasi operasi.

C. Degree Distribution (Distribusi Derajat Keterhubungan)

Derajat keterhubungan merupakan indikator penting untuk menentukan apakah jaringan bersifat tersentralisasi atau terdistribusi. Gambar 2 menunjukkan distribusi nilai *degree centrality* pada semua aktor.



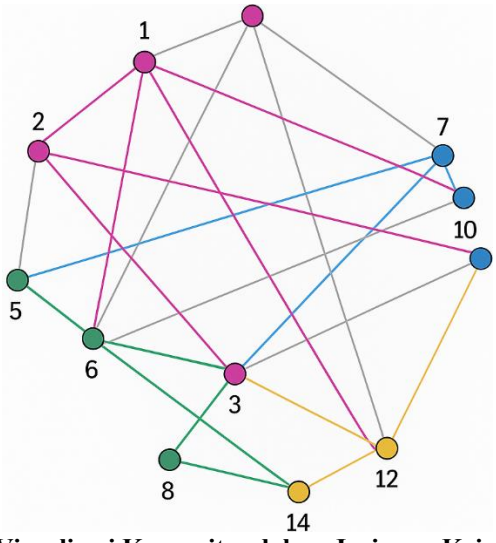
Gambar 2. Distribusi Derajat Keterhubungan Aktor dalam Jaringan
Sumber: Hasil pemrosesan python_user_visible (2025)

Distribusi menunjukkan pola *right-skewed*, di mana sebagian besar aktor memiliki tingkat keterhubungan rendah, sementara hanya sedikit aktor memiliki derajat sangat tinggi. Pola ini

merupakan ciri khas *scale-free network*, yaitu struktur jaringan yang umum ditemukan dalam jaringan kriminal, jaringan terorisme, dan jaringan *darknet*. Pola ini menunjukkan bahwa penindakan terhadap aktor sentral akan memberikan dampak besar terhadap melemahnya jaringan.

D. Community Detection (Deteksi Komunitas dalam Jaringan)

Gambar 3 memvisualisasikan subkelompok (komunitas) dalam jaringan menggunakan algoritma *greedy modularity*. Setiap komunitas direpresentasikan dengan warna node yang berbeda.



Gambar 3. Visualisasi Komunitas dalam Jaringan Kejahatan Siber
Sumber: Hasil pemrosesan python_user_visible (2025)

Komunitas yang teridentifikasi menunjukkan adanya klaster yang saling berhubungan tetapi memiliki fungsi berbeda. Dalam konteks kejahatan siber ASEAN, klaster biasanya dapat mencerminkan *subunit* operasional seperti kelompok pengembang *malware*, kelompok eksekutor serangan, penyedia layanan infrastruktur ilegal, *fasilitator finansial. Node* 0 kembali terlihat berperan sebagai penghubung antarkomunitas, menjadikannya target paling strategis dalam upaya penindakan.

Diskusi

Hasil analisis jaringan memperlihatkan adanya struktur kejahatan siber yang menyerupai ekosistem dengan peran-peran tertentu yang terdistribusi dalam beberapa komunitas. Aktor sentral seperti *Node* 0 memegang kendali atas arus komunikasi dan menjadi titik persimpangan dari berbagai jalur interaksi yang lebih kecil. Hal ini menunjukkan bahwa kelompok kriminal tidak bekerja secara linear, tetapi membentuk jaringan kompleks dengan mekanisme hubungan berlapis. Temuan ini konsisten dengan penelitian (Kant et al., 2025) yang menyatakan bahwa sebagian besar jaringan darknet memiliki *power law distribution*, di mana hanya beberapa aktor memainkan peran dominan. (Rosenquist et al., 2024; Tzanetakis & Marx, 2023) juga menekankan bahwa keberhasilan operasi kriminal digital bertumpu pada struktur sosial jaringan, bukan sekadar kemampuan teknis pelaku. Analisis graf dalam penelitian ini memperkuat argumen tersebut dan memperluasnya pada konteks Asia Tenggara yang memiliki dinamika regulasi lintas negara lebih kompleks.

Secara teoretis, penelitian ini memberikan kontribusi penting terhadap literatur kriminologi digital dengan menunjukkan bahwa pendekatan SNA dapat mengungkap struktur tersembunyi yang tidak dapat diidentifikasi melalui analisis kasus tradisional. Temuan mengenai sifat *scale-free network* dan struktur komunitas memperkuat argumentasi tentang adanya hierarki implisit dalam jaringan kejahatan siber, meskipun secara formal tampak terdesentralisasi. Bagi aparat penegak hukum ASEAN, hasil ini dapat menjadi dasar untuk strategi penindakan yang lebih presisi. Mengarahkan intervensi pada aktor dengan *betweenness centrality* tinggi dapat memutus jalur komunikasi dan melumpuhkan jaringan secara keseluruhan. Temuan struktur komunitas juga dapat membantu mengidentifikasi fungsi teknis masing-masing segmen jaringan.

Penelitian ini menghadapi keterbatasan berupa keterbatasan data empiris otentik yang dapat digunakan secara terbuka. Data sintetis digunakan untuk keperluan visualisasi, sehingga struktur jaringan aktual bisa lebih kompleks. Selain itu, OSINT sering mengandung *noise* informasi, meskipun proses validasi telah dilakukan. Penelitian selanjutnya disarankan menggunakan data real dari instansi penegak hukum atau kerja sama regional ASEAN untuk meningkatkan akurasi pemetaan. Integrasi SNA dengan analisis forensik digital dan analisis temporal jaringan juga akan membuka peluang pemahaman lebih mendalam terhadap dinamika kejahatan siber lintas negara.

IV. KESIMPULAN

Penelitian ini menunjukkan bahwa kejahatan siber terorganisir di kawasan ASEAN memiliki struktur jaringan yang kompleks, adaptif, dan ditopang oleh hubungan sosial antarpelaku yang berperan dalam menjaga keberlangsungan operasi lintas negara. Melalui penerapan *Social Network Analysis,* penelitian ini mampu mengidentifikasi aktor-aktor sentral, jalur komunikasi utama, serta subkomunitas fungsional yang beroperasi dalam jaringan. Temuan seperti dominasi node berpengaruh, adanya struktur *scale-free network*, dan keterhubungan antarkomunitas memperlihatkan bahwa kejahatan siber tidak bekerja secara acak, tetapi melalui pola relasional yang terstruktur. Hal ini menguatkan pemahaman teoretis dalam kriminologi digital bahwa analisis jaringan memberikan perspektif yang lebih komprehensif dibandingkan pendekatan tradisional yang berfokus pada individu atau modus operandi semata.

Secara praktis, hasil penelitian ini menawarkan landasan strategis bagi upaya penanggulangan kejahatan siber di ASEAN. Identifikasi aktor sentral dan titik penghubung dapat menjadi dasar alat bantu pengambilan keputusan dalam operasi penegakan hukum, terutama dalam menentukan target intervensi yang paling efektif untuk melemahkan jaringan. Meski penelitian ini memiliki keterbatasan terkait ketersediaan data empiris dan penggunaan data sintetis untuk visualisasi, temuan yang dihasilkan tetap memberikan kontribusi penting dalam pengembangan kebijakan keamanan siber regional. Ke depan, kolaborasi data antarnegara, integrasi SNA dengan analisis forensik digital, serta pendekatan longitudinal terhadap dinamika jaringan menjadi rekomendasi utama untuk memperkuat pemahaman dan respons terhadap kejahatan siber terorganisir di kawasan ASEAN.

REFERENCES

Abdullah, M., Nawaz, M. M., Saleem, B., Zahra, M., Ashfaq, E. binte, & Muhammad, Z. (2025). Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data. *Analytics*, *4*(3). https://doi.org/10.3390/analytics4030025

Anggoro, F., Caraka, R. E., Prasetyo, F. A., Ramadhani, M., Gio, P. U., Chen, R. C., & Pardamean, B. (2022). Revisiting Cluster Vulnerabilities towards Information and Communication Technologies in the Eastern Island of Indonesia Using Fuzzy C Means. *Sustainability (Switzerland)*, *14*(6). https://doi.org/10.3390/su14063428

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics (Switzerland)*, *12*(6). https://doi.org/10.3390/electronics12061333

Bartlett, B. (2024). Why do States Engage in Cybersecurity Capacity-Building Assistance? Evidence from Japan. *Pacific Review*, *37*(3), 475–503. https://doi.org/10.1080/09512748.2023.2183242

Bright, D., Brewer, R., & Morselli, C. (2022). Reprint of: Using Social Network Analysis to Study Crime: Navigating the Challenges of Criminal Justice Records. *Social Networks*, *69*, 235–250. https://doi.org/10.1016/j.socnet.2022.01.008

Chen, H., Mehra, A., Tasselli, S., & Borgatti, S. P. (2022). Network Dynamics and Organizations: A Review and Research Agenda. *Journal of Management*, *48*(6), 1602–1660. https://doi.org/10.1177/01492063211063218

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, *10*(1). https://doi.org/10.1057/s41599-023-01560-x

Chen, Y., Huang, M., Niu, D., & Wang, J. (2025). The Impact of Digital Trade on Economic Growth and Its Mechanism: Evidence from 60 Countries. *Emerging Markets Finance and Trade*. https://doi.org/10.1080/1540496X.2025.2559940

Dillon, R., & Tan, K.-L. (2024). Cybersecurity Workforce Landscape, Education, and Industry Growth Prospects in Southeast Asia. *Journal of Tropical Futures: Sustainable Business, Governance & Development*, *1*(2), 172–181. https://doi.org/10.1177/27538931231176903

Hemdani, M. G. K. (2025). Cryptocurrencies and the Dark Web: A Gateway to Money Laundering. *Studies in Computational Intelligence*, *1181*, 217–247. https://doi.org/10.1007/978-3-031-80557-8_10

Ho, H. T. N., & Luong, H. T. (2022). Research Trends in Cybercrime Victimization During 2010–2020: A Bibliometric Analysis. *SN Social Sciences*, *2*(1). https://doi.org/10.1007/s43545-021-00305-4

K, H. (2024). Cyber Forensic and Crime Investigation. *LawFoyer International Journal of Doctrinal Legal Research*, *2*(3), 335–364. https://doi.org/10.70183/lijdlr.2024.v02.21

Kant, R., Pal, R., Dixit, A. K., & Kaur, G. (2025). Dark Net and Deep Web: Legal Issues and Regulations. *Lecture Notes in Networks and Systems*, *1408 LNNS*, 557–582. https://doi.org/10.1007/978-981-96-6297-5_42

Karo-Karo, G. F. M., Harumnanda, M. S. A., & Lim, C. (2023). Investigating Multiple Malware as a Service (MaaS): Analysis and Prevention Techniques. *Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges, ICoCICs 2023*, 270–274. https://doi.org/10.1109/ICoCICs58778.2023.10277515

Kuzior, A., Brożek, P., Kuzmenko, O., Yarovenko, H., & Vasilyeva, T. (2022). Countering Cybercrime Risks in Financial Institutions: Forecasting Information Trends. *Journal of Risk and Financial Management*, *15*(12). https://doi.org/10.3390/jrfm15120613

Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure. *Computational Methods in Applied Sciences*, *56*, 3–42. https://doi.org/10.1007/978-3-030-91293-2_1

Liu, J., & Li, F. (2024). Rural revitalization driven by digital infrastructure: Mechanisms and empirical verification. *Journal of Digital Economy*, *3*, 103–116. https://doi.org/10.1016/j.jdec.2025.01.002

Manantan, M. B. (2025). Cyber ASEAN: Advancing Cyber Resiliency and Capacity in Southeast Asia. *The Palgrave Handbook on Cyber Diplomacy*, 905–925. https://doi.org/10.1007/978-3-031-93385-1_42

Mirzaye, S., & Mohiuddin, M. (2025). Digital Transformation in International Trade: Opportunities, Challenges, and Policy Implications. *Journal of Risk and Financial Management*, *18*(8). https://doi.org/10.3390/jrfm18080421

Nicolás-Sánchez, A., & Castro-Toledo, F. J. (2024). Uncovering the Social Impact of Digital Steganalysis Tools Applied to Cybercrime Investigations: A European Union Perspective. *Crime Science*, *13*(1). https://doi.org/10.1186/s40163-024-00209-7

Purba, D. S., Dwi Permatasari, P., Tanjung, N., Rahayu, P., Fitriani, R., Wulandari, S., Universitas,), Negeri, I., Utara, S., Muslim, U., & Al Washliyah, N. (2025). Analisis Perkembangan Ekonomi Digital dalam Meningkatkan Pertumbuhan Ekonomi di Indonesia. *Jurnal Masharif Al-Syariah: Jurnal Ekonomi Dan Perbankan Syariah*, *10*(1). https://doi.org/10.30651/JMS.V10I1.25367

Robertson, C., Bouchard, M., Whelan, C., & Girn, A. (2025). Untangling SNA: The Use and Underuse of Social Network Analysis Among Crime Analysts. *Police Practice and Research*. https://doi.org/10.1080/15614263.2025.2574317

Rosenquist, H., Hasselquist, D., Arlitt, M., & Carlsson, N. (2024). On the Dark Side of the Coin: Characterizing Bitcoin Use for Illicit Activities. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *14538 LNCS*, 37–66. https://doi.org/10.1007/978-3-031-56252-5_3

Scharfman, J. (2024). Wallet Drainers, Crypto Stealers and Cryptojacking. *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II*, 271–306. https://doi.org/10.1007/978-3-031-60836-0_10

Shahriar, S., Allana, S., Hazratifard, S. M., & Dara, R. (2023). A Survey of Privacy Risks and Mitigation Strategies in the Artificial Intelligence Life Cycle. *IEEE Access*, *11*, 61829–61854. https://doi.org/10.1109/ACCESS.2023.3287195

Taherdoost, H. (2025). Insights into Cybercrime Detection and Response: A Review of Time Factor. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5262063

Tzanetakis, M., & Marx, S. A. (2023). The Power of Digital Platforms: What do Darknet Drug Platforms Have in Common with Platform Giants? *Economic Sociology in Europe: Recent Trends and Developments*, 49–69. https://doi.org/10.4324/9781003353560-4

Verma, A. and S. C. (2022). Cyber Security: A Review of Cyber Crimes, Security Challenges and Measuresto Control. *Vision*.

Vogel, J. W., Corriveau-Lecavalier, N., Franzmeier, N., Pereira, J. B., Brown, J. A., Maass, A., Botha, H., Seeley, W. W., Bassett, D. S., Jones, D. T., & Ewers, M. (2023). Connectome-based modelling of neurodegenerative diseases: towards precision medicine and mechanistic insight. *Nature Reviews Neuroscience*, *24*(10), 620–639. https://doi.org/10.1038/s41583-023-00731-8

Yeboah-Ofori, A., & Opoku-Boateng, F. A. (2023). Mitigating Cybercrimes in an Evolving Organizational Landscape. *Continuity & Resilience Review*, *5*(1), 53–78. https://doi.org/10.1108/crr-09-2022-0017

Zreik, M. (2024). Governing Complex Disasters in Southeast Asia: A Focus on COVID-19 Management in Malaysia. *Southeast Asia: A Multidisciplinary Journal*, *24*(3), 171–184. https://doi.org/10.1108/seamj-12-2023-0084