BAB I

PENDAHULUAN

1.1 Latar Belakang

Era digitalisasi 4.0, teknologi telah menjadi kebutuhan mendasar dalam kehidupan manusia, yang menawarkan berbagai macam kemudahan sehingga dapat dimanfaatkan dalam aktivitas sehari-hari. Namun, kemajuan ini juga menghadirkan tantangan baru berupa ancaman serangan siber dibeberapa negera ASEAN. Negara di Asia Tenggara saat ini menjadi sasaran empuk bagi para pelaku kejahatan siber oleh kelompok Lockbit, terutama akibat pesatnya laju digitalisasi di kawasan ini (Subandowo, 2022). LockBit adalah kelompok kejahatan siber berbasis model ransomware-as-a-service (RaaS), di mana operator menyediakan alat, infrastruktur, dan model afiliasi bagi pihak lain untuk melakukan serangan ransomware, sementara afiliasi menjalankan operasional serangan. Kelompok ini muncul sekitar 2019 dengan varian awal "ABCD" ransomware dan kemudian dikenal sebagai LockBit (Tan, Saputri, Xiao, Liu, & Ekeh, 2024).

LockBit berkembang menjadi salah satu ransomware paling aktif di dunia, tercatat menyumbang sekitar 30,25% dari semua serangan ransomware yang diketahui antara Agustus 2021 hingga Agustus 2022 (Kim, Lee, Ramachandran, & Alzahrani, 2025). Karakteristik LockBit meliputi enkripsi data korban sekaligus mencuri data dan mengancam mempublikasikannya jika tebusan tidak dibayar, praktik yang dikenal sebagai "double extortion". Meskipun tidak secara resmi dikaitkan dengan negara tertentu, banyak analisis menunjukkan operator berasal

dari Eropa Timur atau Rusia dan berbahasa Rusia (Couretas, 2024). Ancaman dari LockBit meliputi enkripsi file korban, termasuk dokumen, server, VM, dan infrastruktur TI, sehingga akses menjadi terhalang; eksfiltrasi data pelanggan, pegawai, atau sistem internal yang kemudian diancam atau dipublikasikan jika tebusan tidak dibayar (Couretas, 2024).

Sisi lain, tuntutan tebusan besar dalam bentuk kripto atau uang tunai yang dibagi antara afiliasi dan operator; serangan ke infrastruktur kritis seperti server virtualisasi, sistem backup, Active Directory, lingkungan VMware/ESXi, dan data center; serta ketergantungan model "complex interdependence", di mana satu serangan dapat berdampak luas lintas lembaga dan negara, sehingga menekankan pentingnya kerja sama internasional dan koordinasi institusional (Eliando & Purnomo, 2022). Penggunaan teknologi digital tanpa diimbangi sistem keamanan yang memadai membuka celah besar bagi berbagai bentuk kejahatan siber. Menurut laporan IBM Security, biaya rata-rata yang harus ditanggung oleh organisasi di kawasan ASEAN akibat pencurian data mencapai sekitar USD 2,62 juta, dengan insiden pelanggaran data, rata-rata terdapat 22.500 catatan yang berhasil diretas, sedikit lebih rendah dibandingkan rata-rata global sebesar USD 3,92 juta dengan 25.575 catatan (Pratiwi & Hidayati, 2022).

Berbagai insiden pelanggaran data berskala besar telah tercatat di kawasan negara Singapura, dimana serangan ransomware berhasil menginfeksi data milik sekitar 120.000 orang, termasuk 98.000 anggota Angkatan Bersenjata Singapura (Jayakumar, 2020). Kasus kebocoran data lainnya juga terjadi terhadap 142.000 pasien HIV-positif, dan sebelumnya, sebanyak 1,5 juta data pasien rawat jalan di

Klinik SingHealth juga sempat dibobol oleh peretas (Noriza & Munib, 2023). Sementara itu, di Filipina, lebih dari 80.000 catatan yang memuat informasi pribadi pengguna berhasil diakses oleh peretas setelah situs web Wendy's diretas (Hsiao, Dios, Daroy, & Kalaw-Tirol, 2021). Data yang bocor mencakup informasi sensitif seperti nama, alamat, kata sandi, metode pembayaran, serta riwayat transaksi dan lamaran kerja. Laporan resmi CyberSecurity Malaysia, LockBit tercatat sebagai varian yang mengincar lingkungan server virtualisasi (VMware/ESXi) dan kapasitas backup di Malaysia (Pitchay, Suhaimi, Ridzuan, Ab Halim, & Alwi, 2025). Rentetan insiden ini menegaskan betapa krusialnya penguatan keamanan siber di tengah gelombang digitalisasi yang kian meluas di kawasan Asia Tenggara.

Serangan ransomware kelompok Lockbit 3.0 yang terjadi pada Juni 2024 di Indonesia mengakibatkan gangguan pada berbagai layanan publik di Server Pusat Data Nasional (PDN). Akibat dari peristiwa tersebut, 210 server instansi pemerintah Indonesia terhambat, dan pelaku menuntut biaya pemulihan sebesar 8 juta dollar AS atau 131 miliar (Tommy & Nasution, 2025). Di kawasan ASEAN, sekitar 65% organisasi mengalami serangan ransomware pada tahun 2022, dan 45% dari mereka membayar tebusan. Proyeksi kerugian tahunan akibat ransomware di kawasan ini bisa mencapai sekitar $265 miliar pada tahun 2031, dengan peningkatan biaya tahunan sekitar 30% setiap tahunnya. Ransomware sendiri merupakan malware *(Malicious Software)* yang mengunci atau mengenkripsi data pada sistem korban, sehingga data tidak dapat diakses. Pelaku serangan kemudian meminta tebusan untuk memberikan kunci dekripsi yang

diperlukan untuk memulihkan akses ke data tersebut (Mubarak, Insirat, & Lutfiya, 2024).

Indonesia menjadi target ransomware tertinggi di Asia Tenggara: data dari Kaspersky menunjukkan bahwa Indonesia mencapai 0,25 % pengguna di H1 2025 terkena ancaman ransomware, tertinggi dibanding negara tetangga seperti Malaysia dan Vietnam (Siswanto, 2025). Juni 2024, server Pusat Data Nasional Sementara (PDNS) (Yang dikelola oleh Kementerian Komunikasi dan Informatika Indonesia) dilaporkan terkena serangan ransomware varian "Brain Cipher" yang dilaporkan sebagai mutasi dari LockBit 3.0. Sasaran lebih dari 200 instansi pemerintah pusat/daerah. Tebusan yang diminta sekitar US$ 8 juta (Sunggara & Hariansah, 2024). Mei 2023, Bank Syariah Indonesia (BSI) dilaporkan mengalami serangan dari LockBit 3.0. Kelompok ini mengaku telah mencuri ≈15 juta data nasabah dan karyawan, sekitar 1,5 TB data internal (Aditya Priyatna Darmawan, 2025). Ransomware kelompok Rockbit menyerang server milik Bank Syariah Indonesia di tahun 2023, membuat para nasabah tidak bisa mengakses aplikasi mobile banking selama 5 hari (Solikhawati & Samsuri, 2023).

Platform belanja online Tokopedia juga pernah mengalami pencurian data pengguna akibat ulah hacker, di mana sebanyak 91 juta data pengguna Tokopedia berhasil diretas oleh pihak yang tidak bertanggung jawab meliputi, nama lengkap, tempat tanggal lahir, email, nomor telepon, password hingga aktivitas transaksi (Kusuma & Rahmani, 2022). Serangan DDoS yang menyerang website DPR RI. Serangan yang terjadi tahun 2020 ini menyebabkan website *down* atau tidak bisa

diakses dan nama situs berubah (Ilaina & Nugraha, 2025). Website berita terkemuka Tempo menjadi korban kejahatan *cyber* yang membuat terganggunya layanan pada website, membuat reputasi keamanan Tempo menjadi sorotan karena dianggap sangat rentan (Buana, 2021). Beberapa kasus di atas, yang terjadi di negeri ASEAN, khususnya Indonesia, menegaskan pentingnya penguatan sistem keamanan siber di setiap negara, termasuk kawasan Asia Tenggara.

Serangan LockBit menunjukkan bahwa ancaman siber bersifat lintas negara dan institusional, bukan sekadar lokal, sehingga menekankan pentingnya kerja sama ASEAN melalui inisiatif seperti ACCP. Modus operandi LockBit RaaS dengan enkripsi, eksfiltrasi, dan tuntutan tebusan menunjukkan perlunya kerjasama teknis sekaligus mekanisme kebijakan, regulasi, pertukaran intelijen, dan capacity-building. Karena LockBit menyerang sektor publik, termasuk data pemerintah dan perbankan, serta memanfaatkan teknologi virtualisasi global, negara anggota ASEAN perlu meningkatkan proteksi bersama terhadap infrastruktur kritis dan layanan publik. Kasus di Indonesia dan Malaysia menjadi studi empiris yang relevan untuk menilai peran ACCP, respons nasional, dan bagaimana ASEAN sebagai kerangka institusional menjembatani kerja sama. Keamanan siber menjadi isu krusial yang mempengaruhi stabilitas ekonomi dan keamanan nasional. ASEAN telah memulai berbagai inisiatif seperti ASEAN *Cybersecurity Cooperation Strategy* untuk meningkatkan koordinasi dan kapasitas keamanan siber di Kawasan (Manurung & Finaldin, 2025).

Serangan siber kelompok LockBit tidak hanya berdampak pada sektor teknologi informasi, tetapi juga menimbulkan kerugian besar, seperti yang dialami

ASEAN dengan total kerugian mencapai US$2,87 juta di sektor keuangan akibat serangan siber (IBM, 2022). Menyikapi hal ini, ASEAN sebagai organisasi regional telah menyusun *ASEAN Cybersecurity Cooperation Strategy* sejak tahun 2017 untuk memperkuat keamanan ruang siber secara kolektif. ASEAN berupaya menciptakan ruang siber yang aman, damai, dan tangguh demi mendukung kemajuan ekonomi, konektivitas regional, dan peningkatan kualitas hidup masyarakat Asia Tenggara. Meski dihadapkan pada keterbatasan sumber daya manusia di bidang keamanan siber, kerja sama dengan mitra internasional dan sektor swasta menjadi solusi yang dapat mendorong penguatan kapasitas sumber daya dan pengembangan kerangka hukum serta kebijakan siber yang seimbang antara kepentingan pertahanan nasional dan kemajuan teknologi sebagai sikap optimisme terhadap peningkatan ketahanan dan keamanan siber di Kawasan ASEAN (Pujayanti, Roza, & IP, 2019).

Beberapa tahun terakhir, ancaman siber kelompok kelompok LockBit di dunia maya semakin meningkat karena kekuasaan yang terlalu besar terkonsentrasi pada segelintir individu atau organisasi (Dickson, 2023). Perkembangan dunia maya kekuatan lebih tersebar dan individu memiliki kendali yang lebih besar, kini justru terjadi pergeseran di mana pemerintah, korporasi besar, bahkan kelompok kriminal terorganisir menguasai dan mempengaruhi dunia maya sesuai dengan kepentingannya masing-masing. Dulu awal kemunculan internet, isu keamanan siber belum menjadi perhatian utama bagi sebagian besar perusahaan, negara, maupun organisasi internasional. Mayoritas entitas belum menyadari potensi ancaman yang bisa ditimbulkan oleh dunia maya.

Namun, seiring berjalannya waktu dan semakin maraknya insiden kebocoran data serta serangan siber kelompok LockBit yang menimbulkan dampak besar secara global, kesadaran akan pentingnya *cybersecurity* meningkat tajam.

Beberapa tahun terakhir, kekhawatiran ini semakin nyata karena kekuasaan di dunia maya tidak lagi terdistribusi secara merata, melainkan terkonsentrasi pada segelintir aktor, baik itu negara, perusahaan multinasional, maupun kelompok kriminal terorganisir (Dickson, 2023). Perubahan struktur kekuasaan ini telah menggeser perhatian dunia terhadap urgensi keamanan siber, menjadikannya sebagai prioritas utama dalam agenda global. Dynkin (2018) menyatakan bahwa ancaman siber kelompok LockBit yang terus berkembang secara dinamis telah memaksa perusahaan dan negara untuk beradaptasi melalui pengawasan ketat, pelatihan sumber daya manusia, serta penerapan berbagai kontrol teknis dan prosedural guna memperkuat sistem keamanan mereka. Tidak hanya itu, tren pelanggaran data berskala besar akhir-akhir ini juga mendorong munculnya kekhawatiran terhadap jenis ancaman yang lebih canggih dan spesifik seperti perangkat lunak yang mampu menyusup ke infrastruktur vital negara atau menyerang sejumlah besar target sekaligus.

Maka dalam hal ini, keamanan siber kini bukan lagi pilihan, melainkan suatu keharusan yang melekat dalam tata kelola modern, baik di level korporasi maupun pemerintahan. Perubahan inilah yang mendorong meningkatnya kesadaran global terhadap pentingnya keamanan siber. Kesadaran ini semakin mendalam seiring munculnya pemahaman bahwa *cybersecurity* bukanlah kondisi antara “aman” atau “tidak aman”, melainkan merupakan suatu proses yang

bersifat kontinyu, dinamis, dan berulang. Semua pihak baik negara, organisasi internasional, maupun perusahaan swasta dituntut untuk terus mengembangkan pengetahuan secara bermakna, serta membentuk pemahaman yang lebih jelas mengenai sifat dasar keamanan siber, tujuan dari program-program *cybersecurity* yang adaptif, dan metodologi strategis yang dapat diimplementasikan untuk menciptakan sistem pertahanan dunia maya yang handal dalam menghadapi berbagai bentuk ancaman siber. Ancaman siber atau *cyber threat* sendiri, sebagaimana didefinisikan oleh *Oxford Dictionary* (2018), adalah kemungkinan adanya upaya jahat untuk merusak atau mengganggu jaringan atau sistem komputer.

Menurut *Secureworks* (2017), *cyber threat* merupakan potensi ancaman dari aktor atau pihak tertentu yang mencoba mengakses sistem secara tidak sah dengan tujuan menyusup, mencuri data, atau merusak sistem menggunakan Taktik, Teknik, dan Prosedur (TTP) yang dirancang secara terukur dan spesifik. Ancaman ini dapat berupa virus komputer, pencurian hak kekayaan intelektual, pencurian dana, manipulasi atau penghancuran data, penyadapan melalui perangkat elektronik, hingga bentuk-bentuk pelanggaran digital lainnya. Dengan sifat ancaman yang semakin kompleks dan beragam ini, maka urgensi akan sistem keamanan siber dari kelompok LockBit yang tangguh dan adaptif menjadi semakin nyata dan tak terhindarkan. Banyaknya kerugian yang ditimbulkan akibat serangan siber serta minimnya pemahaman dari negara maupun perusahaan mendorong berbagai pihak untuk melihat pentingnya kerja sama dengan

Menyusun kebijakan-kebijakan tentang keamanan siber di Kawasan ASEAN, sebagai upaya dalam menghadapi ancaman siber pada tahun berikutnya.

Negara-negara di Asia Tenggara bersama dengan organisasi internasional, khususnya organisasi antar-pemerintah seperti *Association of Southeast Asian Nations* (ASEAN), tengah berupaya secara aktif dalam mencari solusi terhadap berbagai tantangan yang muncul dalam ranah keamanan siber. Hal ini disebabkan oleh meningkatnya ancaman digital lintas negara yang tidak hanya mengganggu stabilitas ekonomi, tetapi juga membahayakan keamanan nasional dan regional. Sebagai langkah konkret untuk mengatasi permasalahan tersebut secara kolektif, ASEAN meluncurkan program ASEAN *Cyber Capacity Program* (ACCP) untuk meningkatkan kapasitas negara-negara anggotanya dalam menghadapi ancaman siber, baik dari sisi teknis, kebijakan, maupun sumber daya manusia. ACCP berfungsi sebagai wadah kerja sama regional yang memfasilitasi pertukaran pengetahuan, pelatihan teknis, pembangunan infrastruktur keamanan siber, serta penguatan kebijakan dan regulasi sejalan dengan standar internasional dari sektor swasta dan masyarakat sipil, guna menciptakan ekosistem digital yang lebih tangguh, adaptif, dan aman di kawasan Asia Tenggara.

Kebijakan ini mencakup kerja sama kesiapsiagaan siber melalui pertukaran informasi, penguatan koordinasi regional lewat forum seperti ASEAN Cyber-CC dan AMCC, adopsi standar internasional, pengembangan kapasitas lewat pelatihan dan legislasi, serta perluasan kerja sama internasional yang saling menguntungkan. Meningkatnya ancaman siber kelompok LockBit di kawasan Asia Tenggara mendorong negara-negara termasuk Indonesia untuk memperkuat

kerja sama keamanan melalui ASEAN. Penelitian Attaqi (2021) dan Primawanti & Pangestu (2020) menunjukkan bahwa kebijakan luar negeri Indonesia dalam menanggulangi cybercrime melalui kerja sama regional masih belum maksimal. Sementara itu, Chotimah (2019) dan Rosy (2020) menekankan pentingnya peran kelembagaan seperti BSSN dan diplomasi bilateral-multilateral. Rizki (2022) memperkuat argumen bahwa Indonesia menjadi sasaran utama serangan siber dan mengalami kerugian besar. Hal ini menegaskan perlunya studi lebih lanjut terhadap efektivitas kebijakan luar negeri Indonesia dalam konteks kerja sama regional untuk memperkuat ketahanan siber nasional.

Berbeda dengan penelitian Kannaby (2020), Aurelia (2024), dan Judijanto & Nugroho (2025), sebagian besar masih berfokus pada tataran implementasi kebijakan, peraturan perundangan, dan diplomasi institusional. Namun, belum ada penelitian yang secara spesifik menganalisis efektivitas diplomasi siber kelompok LockBit di Indonesia dalam konteks pembangunan kepercayaan dan penyelarasan strategi keamanan siber antarnegara ASEAN melalui program ACCP. Penelitian-penelitian tersebut juga belum menyoroti bagaimana pendekatan Indonesia sebagai aktor strategis mampu menjembatani kesenjangan teknologi, kapasitas, dan koordinasi yang ada di kawasan. Terdapat celah penting untuk mengeksplorasi kontribusi diplomasi Indonesia terhadap harmonisasi dan penguatan tata kelola keamanan siber regional dari kelompok LockBit secara mendalam.

Penelitian ini bertujuan untuk mengungkap dinamika implementasi kebijakan keamanan siber ASEAN yang dinilai belum sepenuhnya efektif dan

merata dalam menghadapi berbagai ancaman siber kelompok LockBit pada tahun 2024. Penelitian ini menganalisis kepentingan strategis dan dinamika internal kawasan yang memengaruhi pelaksanaan kebijakan tersebut, dengan menyoroti kesenjangan kapabilitas antarnegara anggota serta konsistensi komitmen kolektif ASEAN dalam memperkuat keamanan digital di tingkat regional. Kebaharuan penelitian terdapat pada fokus temporal dan pendekatan analisis kawasan terhadap implementasi kebijakan keamanan siber ASEAN pada tahun 2024 yang belum banyak ditelaah secara mendalam. Berbeda dengan penelitian sebelumnya yang cenderung menyoroti kebijakan secara umum, penelitian ini secara spesifik mengulas dinamika internal kawasan ASEAN, seperti kesenjangan kapabilitas antarnegara anggota, kepentingan strategis nasional, serta efektivitas kerja sama regional.

Selain itu, penelitian ini berusaha membedah konsistensi komitmen kolektif ASEAN dalam menghadapi meningkatnya intensitas dan kompleksitas serangan siber, sekaligus mengevaluasi capaian dan tantangan aktual dari kebijakan keamanan siber dari kelompok LockBit di ASEAN dalam konteks geopolitik dan transformasi digital terbaru. Dengan harapan bahwa meskipun ASEAN telah memiliki kerangka kerja sama dan kebijakan keamanan siber secara regional, implementasinya belum merata dan efektif di seluruh negara anggota. Perbedaan tingkat kesiapan infrastruktur digital, sumber daya manusia, dan kepentingan nasional masing-masing negara masih menjadi hambatan utama dalam memperkuat kolektivitas ASEAN dalam menghadapi ancaman siber kelompok LockBit. Hasil penelitian juga diasumsikan akan menemukan bahwa

terdapat ketimpangan antara komitmen normatif ASEAN dan implementasi praktis di lapangan, yang menuntut perbaikan dalam bentuk harmonisasi kebijakan, peningkatan kapasitas, serta koordinasi yang lebih intensif antaranggota dan mitra strategis. Berdasarkan acuan latar belakang dan tujuan penelitian yang telah di paparakan maka berikut judul penelitian ini "Kerja Sama ASEAN melalui ASEAN Cyber Capacity Program (ACCP) dalam Menghadapi Ancaman Siber oleh Kelompok Lockbit (2023–2025)"

1.2 Rumusan Masalah

"Bagaimana peran institusional ASEAN Cyber Capacity Program (ACCP) sebagai mekanisme kerja sama kolektif dalam menghadapi ancaman siber transnasional oleh kelompok Lockbit pada periode 2023–2025?"

1.3 Tujuan Penelitian

Tujuan penelitian ini sendiri terbagi menjadi dua bagian, yaitu tujuan umum dan tujuan khusus. Kedua jenis tujuan tersebut akan dijelaskan pada subbab berikut.

1.3.1 Tujuan Umum

Penelitian ini bertujuan untuk menganalisis peran institusional dan efektivitas mekanisme kerja sama kolektif ASEAN melalui ASEAN Cyber Capacity Program (ACCP) dalam menghadapi ancaman siber transnasional yang ditimbulkan oleh kelompok Lockbit selama periode 2023–2025.

1.3.2 Tujuan Khusus

Penelitian ini bertujuan untuk menganalisis kepentingan strategis serta dinamika internal kawasan yang memengaruhi implementasi kebijakan keamanan

siber ASEAN dalam merespons meningkatnya intensitas dan kompleksitas ancaman siber di tahun 2024, khususnya dengan menyoroti kesenjangan kapabilitas antarnegara anggota serta konsistensi komitmen kolektif ASEAN terhadap keamanan digital regional.

1.4 Kegunaan Penelitian

1. Mengidentifikasi peran dan kontribusi ASEAN melalui ACCP dalam meningkatkan kapasitas keamanan siber negara-negara anggotanya.
2. Menganalisis dinamika dan tantangan yang dihadapi ASEAN dalam memperkuat kerja sama menghadapi ancaman dari kelompok Lockbit.
3. Mengevaluasi sejauh mana ACCP berkontribusi terhadap peningkatan ketahanan siber kawasan Asia Tenggara pada periode 2023–2025.
4. Memberikan rekomendasi strategis untuk memperkuat efektivitas ACCP dan mempersempit kesenjangan kapabilitas keamanan siber antarnegara anggota ASEAN.

1.4.1 Kegunaan Akademis

Penelitian ini bertujuan untuk mengkaji bentuk dan efektivitas kerja sama ASEAN melalui ASEAN Cyber Capacity Program (ACCP) dalam menghadapi ancaman siber lintas batas yang ditimbulkan oleh kelompok Lockbit, dengan menggunakan kerangka teori Neoliberal Institutionalism. Melalui pendekatan ini, penelitian berupaya menjelaskan bagaimana institusi regional seperti ASEAN berperan sebagai fasilitator kerja sama antarnegara anggota dalam menciptakan aturan, meningkatkan transparansi, serta membangun kepercayaan di bidang keamanan digital.

Penelitian ini diharapkan dapat memberikan kontribusi akademis dalam memperkaya literatur hubungan internasional kontemporer, khususnya kajian tentang kerja sama institusional di kawasan Asia Tenggara dalam menghadapi ancaman keamanan non-tradisional, seperti kejahatan siber. Penelitian ini juga memperkuat relevansi teori Neoliberal Institutionalism dalam konteks diplomasi siber dan tata kelola keamanan regional.

1.4.2 Kegunaan Praktis

Secara praktis, penelitian ini memberikan pemahaman mendalam mengenai efektivitas, tantangan, dan peluang kerja sama ASEAN melalui ACCP dalam memperkuat ketahanan siber regional menghadapi ancaman kelompok Lockbit pada periode 2023–2025. Hasil penelitian ini dapat menjadi referensi bagi pembuat kebijakan di tingkat nasional dan regional untuk menyusun strategi yang lebih terpadu, adaptif, dan kolaboratif dalam menghadapi serangan siber lintas negara.

Selain itu, penelitian ini juga diharapkan dapat menjadi acuan bagi aktor non-negara, seperti sektor swasta, lembaga teknologi, dan masyarakat sipil, dalam memperkuat kesadaran, kapasitas, serta kolaborasi publik–privat di bidang keamanan digital. Penelitian ini memiliki nilai strategis dalam mendukung upaya ASEAN mewujudkan ekosistem siber yang aman, tangguh, dan inklusif di kawasan Asia Tenggara.

1.5 Kerangka Pemikiran Teoritis

1.5.1 Literatur Review

Sebelumnya, sudah terdapat sejumlah penelitian mengenai kebijakan luar negeri Indonesia dalam menanggulangi *cybercrime* melalui kerjasama dengan Negara di ASEAN, termasuk Attaqi, M. F.(2021) dengan metode kualitatif yang menanyakan implementasi kebijakan luar negeri Indonesia dalam menanggulangi *cyber crime* melalu kerjasama dengan ASEAN. Hasil penelitian menunjukkan bahwa kebijakan luar negeri Indonesia dalam melakukan kerjsama untuk mengatasi *cyber crime* masih belum maksimal melihat kasus serangan *cyber* meningkat dari tahun ke tahun.

Penelitian Kannaby, A. H. (2020), dengan metode kualitatif yang menanyakan implementasi ASEAN *Cybersecurity Cooperation Strategy* beroperasi dalam menghadapi ancaman keamanan siber di Asia Tenggara. Hasil penelitian menunjukkan bahwa upaya yang dicanankan ASEAN *Cybersecurity Cooperation* dapat memberikan solusi mengenai permasalahan keamanan siber, meskipun beberapa permasalahan terjadi mulai dari kerja sama internasional yang implementasinya masih belum sempurna, kesenjangan teknologi di negara sendiri maupun dengan negara lain, serta tata kelola teknologi yang belum matang dan merata di masing-masing negara.

Penelitian Aurelia, A.(2024), dengan metode kualitatif yang menanyakan implementasi ASEAN Cyber Security Framework 2017-2020 di Singapura pada tahun 2020. Hasil penelitian menunjukkan bahwa Singapura telah memperkuat posisinya dalam meningkatkan kerjasama dan koordinasi di bidang keamanan

siber melalui berbagai inisiatif seperti Singapore's Safer Cyberspace Masterplan 2020 dan berkolaborasi dengan firma siber sekuritas. Singapura meraih peringkat tertinggi *Global Cybersecurity Index*, meningkatkan ketahanan siber nasional, dan menjadi teladan dalam penerapan ASEAN *Cyber Security Framework* serta berkontribusi besar terhadap pengembangan kerangka keamanan siber yang lebih efektif di kawasan ASEAN.

Penelitian Primawanti, H., & Pangestu, S.(2020). dengan metode kualitatif yang menanyakan mengetahui bagaimana Indonesia dalam berdiplomasi demi meningkatkan keamanan siber melalui ASEAN regional Forum. Hasil penelitian menunjukkan bahwa keadaan *Cybersecurity* Indonesia masih memiliki banyak celah, kepentingan nasional berupa kebutuhan keamanan yang bersifat mutlak dan ancaman-ancaman yang berasal dari ruang siber. Diplomasi ASEAN Regional Forum, Indonesia mengusulkan empat poin khusus melalui perumusan kurikulum dalam peningkatan capacity building, transisi penggunaan *Internet Protocol version* 4 (IPv4) ke IPv6, pembentukan badan atau lembaga khusus terkait *cyber*.

Penelitian Chotimah, H. C.(2019), dengan metode kualitatif yang menanyakan mengenai tata kelola keamanan siber dan diplomasi siber Indonesia di bawah kelembagaan Badan Siber dan Sandi Negara (BSSN). Hasil penelitian menunjukkan bahwa peran BSSN dalam tata kelola keamanan siber di Indonesia sekaligus dalam pelaksanaan diplomasi siber Indonesia baik yang dilakukan melalui kerjasama bilateral maupun multilateral.

Penelitisn Rosy, A. F.(2020), dengan metode kualitatif yang menanyakan mengenai pengembangan kapasitas keamanan siber dan kerja sama internasional

di bidang keamanan siber yang dilakukan Indonesia dengan negara lain. Hasil penelitian menunjukkan bahwa pengembangan keamanan siber Indonesia diperkuat dengan dibentuknya Badan Siber dan Sandi Negara. Diplomasi siber Indonesia telah menghasilkan kerja sama dengan negara lain untuk memperkuat keamanan siber sebagai bagian dari keamanan nasional.

Penelitian Judijanto, L., & Nugroho, B.(2025), dengan metode kualitatif yang menanyakan mengenai peraturan keamanan siber dan mekanisme penegakan hukum di Indonesia dalam menangani kejahatan siber dengan menggunakan pendekatan yuridis normative. Hasil penelitian menunjukkan bahwa adanya kemajuan yang signifikan, termasuk pemberlakuan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Namun, masih ada kesenjangan dalam menangani ancaman yang muncul, ambiguitas dalam ketentuan hukum, dan inefisiensi penegakan hukum karena sumber daya yang terbatas dan masalah koordinasi.

Penelitian Rizki, M.(2022), dengan metode kualitatif yang menanyakan mengenai ancaman dan serangan siber menjadi tantangan bagi dunia pertahanan di era sekarang dan bagaimana perkembangan sistem pertahanan dan keamanan siber yang dimiliki oleh Indonesia. Hasil penelitian menunjukkan bahwa serangan siber secara nyata telah memberikan dampak yang besar bagi negara terserang, terkhusus Indonesia, berdasarkan data yang ada telah menjadi negara dengan urutan tertinggi menjadi sasaran penyerangan siber oleh para hacktivist. Total kerugian yang sangat besar patut menjadi sebuah bahan evaluasi bagi bidang keamanan dan pertahanan terkhsusus pada bagian cyberspace.

1.5.2 State of the Art

Berbagai penelitian terdahulu mengenai keamanan siber di kawasan ASEAN telah banyak dilakukan, terutama yang menyoroti kebijakan luar negeri Indonesia dalam menangani kejahatan siber melalui kerja sama regional. Fokus penelitian-penelitian tersebut umumnya mencakup implementasi strategi nasional, efektivitas kerja sama antarnegara ASEAN, serta peran lembaga seperti Badan Siber dan Sandi Negara (BSSN) dalam diplomasi dan penguatan kapasitas keamanan siber. Namun demikian, sebagian besar studi tersebut masih berfokus pada aspek internal kebijakan Indonesia atau meninjau instrumen kerja sama ASEAN secara umum tanpa membahas secara mendalam inisiatif spesifik seperti ASEAN Cyber Capacity Program (ACCP).

Selain itu, belum terdapat penelitian yang menelaah secara langsung bagaimana ACCP berperan sebagai instrumen kolektif ASEAN dalam menghadapi ancaman siber yang bersifat lintas negara, khususnya serangan dari kelompok Lockbit yang menjadi salah satu aktor siber paling aktif di kawasan sejak 2023. Dengan demikian, terdapat celah penelitian (research gap) yang signifikan, yaitu kurangnya kajian yang mengaitkan antara kebijakan luar negeri Indonesia, dinamika kerja sama ASEAN melalui ACCP, dan respons terhadap ancaman siber aktual seperti Lockbit. Oleh karena itu, penelitian ini hadir untuk mengisi kekosongan tersebut dengan menelaah arah serta implementasi kerja sama siber ASEAN melalui ACCP dalam menghadapi ancaman siber oleh kelompok Lockbit selama periode 2023–2025.

1.5.3 Neoliberal Institutionalism Theory

Neoliberal institusionalisme merupakan salah satu pendekatan dalam teori tradisional Hubungan Internasional yang berakar dari pandangan liberal. Teori ini dikembangkan oleh Robert Keohane, yang menekankan bahwa keberadaan institusi internasional memungkinkan terbentuknya kerja sama yang lebih efektif dan berkelanjutan antarnegara. Institusi internasional dipandang sebagai aktor independen yang memiliki peran penting dalam tatanan global. Institusi ini dapat berbentuk organisasi formal seperti NATO atau Uni Eropa, maupun pengaturan dan kesepakatan antarnegara (Jackson & Sorensen, 2007). Neoliberal institusionalisme mendukung kerja sama antarnegara dengan pendekatan yang bersifat ilmiah dan behavioralistis, yakni dengan menitikberatkan pada perilaku dan kepentingan rasional dari aktor-aktor yang terlibat dalam proses kerja sama internasional.

Kaum neoliberal institusionalis berpandangan bahwa negara tetap merupakan aktor utama dalam studi Hubungan Internasional, namun bukan satu-satunya. Aktor non-negara, seperti organisasi internasional, perusahaan multinasional, maupun organisasi masyarakat sipil, juga memainkan peran penting dalam membentuk dinamika kerja sama global. Menurut Jackson dan Sørensen (2024), dijelaskan bahwa meskipun negara memiliki posisi sentral dalam membangun hubungan dan kerja sama internasional, setiap negara tetap berorientasi pada kepentingan nasionalnya. Situasi ini berpotensi menimbulkan ketidakseimbangan, di mana tidak semua negara mendapat manfaat yang sama, sehingga membuka kemungkinan terjadinya konflik akibat persaingan

kepentingan. Hal ini senada dengan asumsi dalam teori realisme, yang menyatakan bahwa negara akan selalu berusaha membangun kekuatan (power) untuk mempertahankan kepentingannya. Oleh karena itu, dalam pandangan kaum realis, kerja sama antarnegara dianggap sulit tercapai karena adanya dorongan kompetitif dan rasa saling curiga.

Keberadaan institusi internasional memainkan peran penting dalam membantu negara-negara yang sedang menghadapi krisis, kerusuhan, bencana, atau kesulitan lainnya. Dalam situasi seperti itu, negara sering kali tidak mampu menangani masalah secara mandiri, salah satunya karena keterbatasan sumber daya dan tingginya biaya penanganan. Neoliberalisme institusional hadir dengan menawarkan solusi melalui penguatan kerja sama internasional. Mengacu pada pandangan Keohane dan Nye (2003), bentuk kerja sama yang dimaksud terjadi dalam konteks ketergantungan kompleks *(complex interdependence)*, yaitu situasi di mana baik aktor negara maupun non-negara saling bergantung satu sama lain. Kebijakan dan tindakan yang diambil oleh satu aktor akan menimbulkan dampak terhadap aktor lainnya. Selanjutnya, Keohane (2003), menekankan bahwa kerja sama internasional hanya dapat terwujud apabila para aktor mampu menghadapi dan menyelesaikan permasalahan bersama secara kolektif, serta berkomitmen untuk menghindari praktik curang yang berpotensi mengganggu stabilitas dan keberlanjutan hubungan kerja sama tersebut.

Keamanan siber (cybersecurity), teori ini relevan karena ancaman siber bersifat lintas batas dan memerlukan kerja sama multilateral. Negara tidak mampu sepenuhnya mengatasi ancaman siber (cyber threats) seperti serangan

ransomware, peretasan infrastruktur kritis, atau spionase siber secara sendiri. Institusi internasional, baik berupa organisasi formal (misalnya ASEAN Cybersecurity Cooperation, NATO Cyber Defense Center) maupun kesepakatan bilateral/multilateral, menjadi sarana untuk memperkuat kemampuan kolektif negara dalam menghadapi ancaman ini.

1. Cybersecurity – Upaya proteksi terhadap sistem informasi, data, dan infrastruktur digital. Neoliberal institutionalism melihat keamanan siber bukan sekadar isu nasional, tetapi sebagai kepentingan bersama yang membutuhkan aturan dan mekanisme institusional untuk memastikan stabilitas global.
2. Cyber Threat – Ancaman terhadap aset digital yang dapat bersifat kriminal, politik, atau ekonomi. Ketergantungan kompleks (complex interdependence) menjelaskan bahwa tindakan satu negara, misalnya mengembangkan kemampuan serangan siber, akan berdampak pada keamanan negara lain, sehingga mendorong perlunya mekanisme koordinasi.
3. Cyber Cooperation – Bentuk kerja sama internasional untuk mencegah, mendeteksi, dan menanggulangi serangan siber. Dalam kerangka neoliberal institusionalisme, cyber cooperation diwujudkan melalui:
    a. Standar dan regulasi keamanan siber bersama.
    b. Pertukaran informasi tentang ancaman dan insiden siber.
    c. Latihan dan simulasi keamanan siber antarnegara.
    d. Bantuan teknis dan kapasitas pembangunan (capacity building) bagi negara-negara dengan keterbatasan sumber daya.

Pandangan Keohane dan Nye (2003), keberhasilan kerja sama ini tergantung pada komitmen kolektif aktor-aktor yang terlibat untuk menghindari praktik curang (cheating) dan menjaga kepercayaan. Institusi internasional bertindak sebagai mediator dan fasilitator, mengurangi risiko konflik dan memastikan bahwa kepentingan nasional tetap selaras dengan kepentingan global dalam menghadapi ancaman siber. Neoliberal institusionalisme memberikan kerangka analisis rasional dan struktural untuk memahami bagaimana negara dan aktor non-negara dapat membangun kerja sama siber yang berkelanjutan. Konsep cybersecurity, cyber threat, dan cyber cooperation berfungsi sebagai variabel operasional yang menjembatani teori dengan praktik nyata di tatanan global.

1.6 Konsep Operasional

1.6.1 Implementasi Kebijakan

Implementasi kebijakan merupakan tahap penting dalam proses kebijakan publik yang berfokus pada bagaimana kebijakan yang telah dirumuskan dijalankan di lapangan. Menurut Van Meter dan Van Horn (1975), implementasi kebijakan adalah tindakan-tindakan yang dilakukan oleh individu, pejabat, atau lembaga pemerintah dalam rangka mencapai tujuan yang telah ditetapkan dalam keputusan kebijakan. Keberhasilan implementasi dipengaruhi oleh beberapa faktor seperti standar dan tujuan kebijakan, sumber daya, komunikasi antar pelaksana, serta kondisi sosial, politik, dan ekonomi yang mendasarinya.

Implementasi kebijakan keamanan siber mengacu pada bagaimana negara-negara anggota ASEAN menerjemahkan berbagai kesepakatan dan strategi regional, seperti ASEAN Cybersecurity Cooperation Strategy serta ASEAN

Digital Masterplan 2025, ke dalam tindakan nyata di tingkat nasional. Hal ini mencakup perumusan program, kebijakan, dan mekanisme koordinasi yang konkret dan terukur untuk memperkuat ketahanan siber masing-masing negara dalam menghadapi ancaman siber yang semakin kompleks di kawasan.

1.6.2 Keamanan Siber

Keamanan siber *(cyber security)* merupakan sistem proteksi yang dirancang untuk menjaga jaringan dan sistem komputer dari berbagai bentuk kejahatan digital seperti virus, pencurian data, peretasan, dan serangan siber lainnya (Sudirman et al., 2024). Keamanan siber *(cybersecurity)* merujuk pada upaya untuk melindungi sistem informasi, jaringan, dan data digital dari gangguan, kerusakan, atau akses tidak sah. Menurut *National Institute of Standards and Technology* (NIST), keamanan siber melibatkan perlindungan terhadap kerahasiaan, integritas, dan ketersediaan informasi yang diproses, disimpan, dan dikirim melalui sistem komputer dan jaringan komunikasi (Wibowo, Nishom, & Abidin, 2024). Perlindungan terhadap jaringan dan sistem ini menjadi aspek yang sangat penting karena menyangkut keamanan informasi pribadi maupun rahasia yang dimiliki oleh pengguna (Schatz & Bashroush, 2017).

Menurut Barry Buzan (2020) memperluas konsep keamanan menjadi dua ranah, yakni keamanan tradisional dan keamanan non-tradisional. Keamanan non-tradisional merujuk pada kondisi bebas dari ancaman yang tidak semata-mata berasal dari konflik militer atau agresi langsung antarnegara. Oleh karena itu, isu keamanan siber dikategorikan sebagai bagian dari keamanan non-tradisional, karena ancaman yang ditimbulkannya tidak bersifat militer konvensional, namun

tetap berpotensi membahayakan individu, negara, maupun organisasi internasional (Buzan, Wæver, & De Wilde, 1998). Terdapat beberapa aspek penting dalam keamanan jaringan atau sistem komputer yang termasuk dalam ruang lingkup *Cyber Security*, antara lain.

1. Perlindungan Kerahasiaan Data

Perlindungan kerahasiaan data bertujuan untuk menjaga informasi dan data agar tetap bersifat rahasia serta tidak dapat diakses oleh pihak yang tidak berwenang. Contoh bentuk data yang harus dijaga kerahasiaannya meliputi kata sandi, informasi pribadi, dan data sensitif lainnya.

2. Proses Verifikasi

Verifikasi merupakan mekanisme pengamanan yang memastikan bahwa individu yang mengakses sistem adalah pengguna yang sah. Hal ini dilakukan untuk mencegah akses dari pihak tidak dikenal, termasuk robot atau entitas otomatis lainnya.

3. Menjaga Integritas Data

Integritas mengacu pada perlindungan data agar tidak mengalami manipulasi, perubahan, penyisipan, pencurian, atau penghapusan oleh pihak yang tidak bertanggung jawab. Tujuannya adalah memastikan bahwa data tetap utuh dan tidak disalahgunakan, sehingga pengguna tidak dirugikan.

Selain aspek-aspek dasar yang telah disebutkan, terdapat pula komponen keamanan lainnya yang perlu dirancang dan diterapkan secara menyeluruh dalam sistem keamanan siber *(cyber security)*. Sistem ini tidak hanya berfungsi untuk melindungi jaringan, tetapi juga mencakup perlindungan terhadap berbagai jenis

perangkat seperti komputer, ponsel pintar, server, sistem elektronik, hingga basis data (database) (Santoso, 2023). Untuk meningkatkan efektivitas perlindungan tersebut, sistem keamanan siber biasanya dibagi ke dalam beberapa kategori utama. Setiap kategori mengklasifikasikan jenis-jenis sistem keamanan komputer yang dibutuhkan sesuai dengan karakteristik ancaman yang dihadapi. Adapun klasifikasi tersebut meliputi:

1. Perlindungan Perangkat Lunak *(Software Security)*

Merujuk pada pengembangan perangkat lunak yang bertujuan utama untuk menjaga sistem komputer dari berbagai bentuk ancaman digital seperti virus, peretasan, pencurian data, dan sebagainya. Contoh dari perlindungan ini meliputi penggunaan antivirus, firewall, serta kontrol akses.

2. Perlindungan Jaringan *(Network Security)*

Kategori ini mencakup langkah-langkah perlindungan terhadap jaringan, terutama yang beroperasi di dunia maya *(cyberspace)* dan terhubung melalui internet. Tujuannya adalah untuk mencegah berbagai serangan seperti malware, penyusupan *(breach),* dan ancaman digital lainnya.

3. Keamanan Informasi *(Information Security)*

Berfokus pada perlindungan data dan informasi pribadi pengguna, baik saat data sedang digunakan, disimpan, maupun dikirimkan. Keamanan ini biasanya diterapkan melalui kebijakan dan prosedur yang sistematis.

4. Keamanan Sistem Operasi *(Operating System Security)*

Mengacu pada perlindungan terhadap sistem operasi yang berjalan dalam perangkat keras. Artinya, sistem operasi seperti Windows perlu dilengkapi dengan

fitur keamanan contohnya Windows Defender untuk memastikan perangkat keras tetap aman saat menjalankan berbagai program.

5. Keamanan Perangkat Keras *(Hardware Security)*

Meliputi perlindungan fisik terhadap perangkat keras dari ancaman langsung. Contoh mekanisme keamanan ini termasuk USB dongle, yang bisa digunakan untuk mencegah virus yang menyebar melalui sambungan USB, serta perangkat akses jarak jauh yang memungkinkan pengoperasian perangkat keras secara eksternal namun tetap aman.

6. Pendidikan Keamanan Pengguna *(User Security Education)*

Aspek ini menekankan pentingnya peningkatan pemahaman pengguna mengenai potensi bahaya dalam dunia siber, seperti virus, peretasan (hacking), dan phishing. Melalui edukasi yang memadai, pengguna dapat lebih waspada dan mampu mencegah terjadinya kejahatan siber.

Ancaman kejahatan siber *(cybercrime)*, sebagai tindakan melanggar hukum yang dilakukan oleh individu maupun kelompok yang tidak bertanggung jawab, baik untuk mendapatkan keuntungan pribadi maupun semata-mata untuk merugikan pihak lain (Fadli, Widijowati, & Andayani, 2024). Dampak dari serangan ini sangat luas, mulai dari pengguna individu hingga mengancam stabilitas dan keamanan suatu negara. Oleh karena itu, diperlukan adanya kebijakan keamanan siber yang mampu memberikan perlindungan dari serangan cybercrime. Selain itu, keamanan siber harus didukung oleh kerangka kebijakan dan regulasi hukum yang disusun oleh pemerintah, organisasi regional, maupun internasional. Pemerintah sendiri memegang peranan penting dalam

menanggulangi dan mencegah kejahatan siber demi menjaga keamanan nasional dan perlindungan terhadap konstitusi negara (Ginanjar, 2022).

Konsep ini membantu menjelaskan bagaimana sebuah negara dapat mempersiapkan diri dalam membangun sistem keamanan siber guna melindungi kedaulatannya, sekaligus mengatur perilaku warganya dalam memanfaatkan teknologi internet di dalam wilayahnya. Hal ini penting karena ruang siber *(cyberspace)* merupakan lingkungan terbuka yang digunakan untuk mengelola dan menyebarkan berbagai jenis informasi (Aji, 2023). Oleh karena itu, setiap negara perlu memiliki strategi serta kebijakan yang terstruktur guna memperkuat sistem pertahanannya, terutama dalam menjaga dan mengamankan teknologi informasi dan komunikasi (ICT) yang menjadi infrastruktur utama bagi pengelolaan basis data nasional. Keamanan siber di negara ASEAN menjadi bagian dari keamanan non-tradisional yang semakin penting seiring meningkatnya digitalisasi dan integrasi ekonomi digital di kawasan.

Keamanan siber tidak hanya mencakup aspek teknis, tetapi juga aspek regulatif dan diplomasi antarnegara, karena potensi ancamannya bersifat lintas batas dan melibatkan aktor negara maupun non-negara. Implementasi ASEAN *Cybersecurity Cooperation Strategy* (ACCS) dapat diidentifikasi dan diklasifikasikan sebagai kebijakan-kebijakan keamanan yang harus diterapkan baik oleh Indonesia maupun negara ASEAN, secara spesifik ditujukan untuk memperkuat sistem keamanan siber. Cybersecurity sebagai implementasi kebijakan ASEAN *Cyber Capacity Program* (ACCP) yang menjadi indikator konkret dari upaya ASEAN membangun ketahanan digital kolektif. Mengacu

pada dokumen ASEAN *Cyber Capacity Program* (2023–2025) dan teori kelembagaan neoliberalis, pengukuran dilakukan berdasarkan tiga dimensi utama:

1. Penguatan Kapasitas Kelembagaan

Fokus pada peningkatan kemampuan teknis, sumber daya manusia, dan infrastruktur digital negara anggota melalui pelatihan, pembentukan lembaga keamanan siber, serta kerja sama teknis. Upaya ini bertujuan memperkecil kesenjangan kemampuan siber antarnegara ASEAN.

2. Harmonisasi Kebijakan Regional

Merujuk pada penyelarasan regulasi dan strategi keamanan siber antarnegara ASEAN melalui ACCP, seperti perlindungan data, *threat intelligence sharing*, dan sistem peringatan dini. Tujuannya menciptakan standar dan kepercayaan bersama di kawasan.

3. Respons terhadap Ancaman Siber Global (Lockbit)

Menunjukkan kemampuan kolektif ASEAN menghadapi serangan ransomware lintas batas dengan koordinasi teknis, berbagi informasi, dan mitigasi ancaman bersama melalui ACCP. Ini menjadi indikator efektivitas kerja sama keamanan siber regional.

1.6.3 Ancaman Siber (*Cyber Threats*)

Ancaman siber merupakan potensi bahaya yang diperkirakan dapat menyebabkan kerugian, gangguan, maupun serangan terhadap keamanan informasi, khususnya yang berkaitan dengan aspek kerahasiaan, integritas, dan ketersediaan data serta sistem teknologi informasi. Klasifikasi ancaman siber umumnya disesuaikan dengan objek atau entitas yang menjadi sasaran utama dan terkena dampak secara langsung (Hoshmand & Ratnawati, 2023). Ancaman siber

(cyberthreat) dipahami sebagai tindakan, gangguan, atau serangan yang dapat merusak atau mengganggu suatu sistem, dengan dampak terhadap aspek kerahasiaan, integritas, maupun ketersediaan data atau layanan. Sumber ancaman siber berasal dari berbagai entitas yang memiliki motif dan kecenderungan untuk melakukan tindakan yang melanggar hukum maupun norma keamanan informasi, baik demi keuntungan material maupun non-material melalui pemanfaatan ruang siber (Ismail et al., 2022).

Entitas atau aktor tersebut dapat berasal dari lingkungan internal maupun eksternal, mencakup intelijen, individu yang mengalami kekecewaan institusional, pihak-pihak yang menjalankan investigasi tidak sah, organisasi ekstremis, kelompok hacktivis, jaringan kejahatan terorganisir, hingga kompetitor dalam konteks persaingan ekonomi dan aktor negara dalam situasi konflik geopolitik. Selain itu, perkembangan teknologi juga turut menjadi faktor yang memperbesar kemungkinan terjadinya pelanggaran keamanan siber (Munajat & Yusuf, 2024). Ruang lingkup ancaman ini meliputi dimensi ideologis, politik, ekonomi, budaya, pertahanan, serta ilmu pengetahuan dan teknologi. Tidak hanya terbatas pada kepentingan negara, ancaman siber juga dapat mengganggu stabilitas masyarakat dan kepentingan individu. Setiap individu maupun institusi, termasuk organisasi pemerintahan dan non-pemerintahan, memiliki potensi untuk menjadi baik subjek maupun objek dari suatu ancaman siber (Azzani, Purwantoro, & Almubaroq, 2023).

Berdasarkan Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, ancaman terhadap pertahanan nasional mencakup dua jenis utama, yaitu

ancaman militer dan non-militer, yang di dalamnya termasuk pula ancaman di ranah siber. Untuk menilai kinerja lembaga pertahanan siber, diperlukan pemahaman yang menyeluruh mengenai bentuk-bentuk ancaman dan serangan digital, serta bagaimana cara mengidentifikasi dan menilai risiko yang mungkin terjadi (Lubis, 2024). Oleh sebab itu, identifikasi potensi serangan dan ancaman dalam dunia maya menjadi dasar dalam menyusun prosedur dan strategi guna mengukur efektivitas organisasi pertahanan siber dalam menangani serta meminimalisir dampak dari berbagai serangan siber (Putra & Supartono, 2018). Ancaman siber *(cyber threats)* mencakup segala bentuk potensi serangan digital yang dapat merusak, mengakses, atau mencuri data dan informasi penting.

Ancaman ini dapat berupa *malware, ransomware, phishing, cyber espionage*, hingga serangan pada infrastruktur kritis seperti sistem perbankan, transportasi, atau jaringan energi (Yuniarti, Alfarizy, Siallagan, & Rizkyanfi, 2023). Ancaman siber bersifat dinamis, kompleks, dan berkembang cepat, sehingga menuntut respons yang adaptif dari pemerintah dan masyarakat. Aspek ancaman siber mencakup berbagai faktor yang menjadi latar belakang terjadinya ancaman maupun serangan siber. Faktor-faktor ini meliputi dimensi ideologi, politik, ekonomi, sosial, budaya, kebangsaan, militer, ilmu pengetahuan, keuangan, dan teknologi, serta elemen-elemen lain yang berkaitan dengan kehidupan berbangsa, bernegara, dan bermasyarakat, termasuk pula kepentingan individu (Sri Yanto et al., 2024). Sebagaimana di jelaskan dalam buku *Pedoman Keamanan Siber Bagi Penyelenggara Inovasi Teknologi Sektor Keuangan* (2024), bahwa terdapat berbagai bentuk ancaman siber yang umum terjadi antara lain:

1. *Malware*

Merupakan perangkat lunak berbahaya yang dirancang untuk mengganggu sistem informasi. Malware bisa menyebabkan kerusakan atau kerugian bagi pemilik sistem, baik secara langsung maupun tidak langsung.

2. *Ransomware*

Jenis malware ini mengenkripsi data milik korban dan meminta tebusan agar data tersebut dapat diakses kembali. Ransomware seringkali berdampak besar secara finansial bagi individu maupun organisasi.

3. *Web Defacement*

Merupakan aksi penyerangan terhadap situs web dengan mengganti tampilan atau kontennya. Perubahan ini dilakukan tanpa izin dan biasanya mencerminkan pesan yang diinginkan oleh pelaku.

4. *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS)

Jenis serangan ini bertujuan mengacaukan sistem elektronik agar tidak dapat diakses oleh pengguna yang sah. Tekniknya adalah dengan membanjiri jaringan atau server dengan permintaan dalam jumlah besar hingga kapasitasnya penuh dan sistem menjadi tidak responsif.

5. *Phishing*

Taktik penipuan yang digunakan untuk mencuri data pribadi seperti username, kata sandi, atau informasi keuangan. Biasanya dilakukan melalui email, pesan teks, atau situs palsu yang menyerupai situs asli.

6. *Social Engineering*

Upaya manipulasi psikologis yang bertujuan membujuk korban untuk melakukan tindakan berbahaya, seperti membagikan data sensitif, mengklik tautan berbahaya, atau mentransfer dana.

7. *Man-in-the-Middle* (MitM)

Jenis serangan di mana pelaku menyusup ke dalam komunikasi antara dua pihak tanpa diketahui. Tujuannya bisa mencuri informasi, mengubah isi pesan, atau mengacaukan komunikasi.

8. *Zero-Day Attack*

Merupakan serangan yang memanfaatkan celah keamanan pada perangkat lunak yang belum diketahui atau belum ditambal oleh pengembang. Karena belum tersedia solusi atau pembaruan, serangan ini sulit untuk dideteksi.

9. Cyber Espionage (Spionase Siber)

Melibatkan pencurian informasi rahasia, baik dari sektor pemerintahan, bisnis, maupun organisasi lainnya. Biasanya dilakukan oleh peretas profesional yang disponsori negara atau kelompok kriminal terorganisir.

10. *Supply* Chain *Attack*

Serangan ini menyasar rantai pasok atau pihak ketiga yang memiliki hubungan dengan target utama. Melalui celah di vendor atau mitra, peretas dapat mengakses sistem dan data organisasi yang lebih besar.

11. *Credential Stuffing*

Merupakan serangan yang menggunakan kombinasi nama pengguna dan kata sandi hasil pencurian (dari kebocoran data, phishing, atau malware) untuk mengakses akun daring milik individu atau organisasi.

Serangan siber seperti penyusupan dan kebocoran informasi melalui jaringan komunikasi harus ditanggapi secara serius. Jika tidak diantisipasi, potensi ancaman ini dapat berkembang menjadi serangan siber yang mampu merusak, mencuri, atau memodifikasi sistem informasi yang vital (Ariyana, Ningtyas, Fauzi, & Ramadhan, 2023). Serangan semacam ini, terutama jika terjadi dalam skala besar dan terkoordinasi, dapat mempengaruhi stabilitas serta ketahanan nasional suatu negara anggota ASEAN. Oleh karena itu, penanganan terhadap ancaman siber perlu didasarkan pada kebijakan keamanan siber yang kuat dan terintegrasi, sebagaimana yang diupayakan dalam *ASEAN Cybersecurity Cooperation Strategy* (ACCS). Kebijakan keamanan siber ASEAN secara kolektif, yang tidak hanya melibatkan negara, tetapi juga aktor non-negara untuk melindungi infrastruktur digital penting dan memastikan keamanan informasi di kawasan Asia Tenggara, khususnya Indonesia. Bagi kawasan seperti ASEAN, yang memiliki tingkat kesiapan dan infrastruktur digital yang bervariasi, ancaman siber menjadi tantangan bersama yang memerlukan respons kolektif dan peningkatan kapasitas keamanan siber nasional serta regional.

1.7 Argumen Penelitian

Penelitian ini berargumen bahwa pada dasarnya, ASEAN melalui kerja sama keamanan siber terus mendorong penguatan kolaborasi antar negara anggotanya untuk menghadapi ancaman siber yang semakin kompleks, sebagai bagian dari kepentingan bersama dalam menciptakan *favorable regional cyber order*. Meskipun masing-masing negara anggota memiliki kepentingan nasional tersendiri, implementasi kebijakan keamanan siber ASEAN lebih diarahkan pada

upaya menjaga stabilitas dan keamanan kawasan di ruang siber. Stabilitas kawasan ini menjadi prioritas dalam menghadapi potensi gangguan, baik dari aktor negara maupun non-negara, yang dapat mengancam tatanan keamanan digital di Asia Tenggara. Oleh karena itu, ASEAN menempatkan terciptanya tatanan keamanan siber yang stabil sebagai prioritas utama dalam agenda kerja samanya.

1.8 Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian kualitatif. Metode penelitian kualitatif merupakan pendekatan yang berfokus pada pemahaman mendalam terhadap suatu kejadian atau peristiwa. Dalam konteks penelitian kualitatif, penekanan diberikan pada penggalian makna, interpretasi, dan pemahaman mendalam terhadap fenomena yang diteliti. Menurut Hancock (2014), penelitian kualitatif bertujuan untuk mencari dan menjelaskan sebab-akibat dari suatu fenomena tertentu. Penulis menggunakan metode kualitatif untuk menjelaskan secara mendalam bagaimana kepentingan strategis nasional dan dinamika kawasan memengaruhi implementasi kebijakan keamanan siber ASEAN, khususnya dalam melihat kesenjangan antarnegara anggota meskipun telah ada komitmen kolektif menghadapi ancaman siber tahun 2024.

1.8.1 Tipe Penelitian

Penelitian ini tergolong ke dalam tipologi eksplanatif. Penelitian eksplanatif merupakan jenis penelitian yang bertujuan untuk memberikan penjelasan mengapa suatu hal terjadi (2010). Penelitian ini bersifat eksplanatif

dengan tujuan utama menjawab pertanyaan “mengapa” implementasi kebijakan keamanan siber ASEAN masih menunjukkan kesenjangan antarnegara anggota, meskipun telah ada komitmen kolektif menghadapi ancaman siber pada tahun 2024. Melalui pendekatan ini, penelitian berupaya mengkaji hubungan antara dinamika kawasan, kepentingan strategis nasional, dan kesenjangan kapabilitas digital guna memahami faktor-faktor yang memengaruhi efektivitas kebijakan keamanan siber di tingkat regional.

1.8.2 Situs Penelitian

Situs penelitian dalam studi ini merujuk pada ruang lingkup kajian yang berfokus pada desk research, yaitu penelitian yang dilakukan dengan menghimpun dan menganalisis data serta literatur yang relevan dari berbagai sumber teks, baik fisik maupun digital. Pendekatan ini dipilih untuk menelusuri dinamika implementasi kebijakan keamanan siber ASEAN dalam menghadapi ancaman siber tahun 2024, dengan memanfaatkan dokumen kebijakan, laporan resmi, publikasi akademik, dan sumber daring lainnya sebagai bahan analisis utama.

1.8.3 Subjek Penelitian

Subjek dalam penelitian ini adalah negara di wilayah ASEAN sebagai aktor regional yang menginisiasi dan melaksanakan kebijakan keamanan siber kolektif di kawasan Asia Tenggara. Sementara itu, objek yang diteliti adalah implementasi kebijakan keamanan siber ASEAN dalam menghadapi ancaman siber yang semakin kompleks di tahun 2024, dengan menyoroti kesenjangan kapabilitas antarnegara anggota serta konsistensi komitmen kolektif dalam kerja sama regional di bidang keamanan digital.

1.8.4 Jenis Data

Penelitian ini menggunakan metode kualitatif, maka jenis data yang digunakan terdiri dari data primer dan data sekunder. Data primer dalam penelitian ini mencakup dokumen resmi, pernyataan kebijakan, dan laporan ASEAN terkait keamanan siber. Sementara itu, data sekunder diperoleh dari literatur akademik, artikel jurnal, laporan lembaga internasional, serta sumber digital yang membahas implementasi kebijakan keamanan siber ASEAN dan kesenjangan antarnegara anggota dalam menghadapi ancaman siber di tahun 2024.

1.8.5 Sumber Data

Analisis dalam penelitian ini didasarkan pada pengumpulan data primer dan sekunder dari sumber-sumber yang kredibel dan relevan. Data primer diperoleh melalui wawancara dengan pihak-pihak yang memahami implementasi kebijakan keamanan siber ASEAN, baik secara daring maupun luring, serta melalui penelusuran informasi mengenai aktor-aktor kunci dalam kerja sama keamanan siber di kawasan. Sementara itu, data sekunder diperoleh melalui studi pustaka terhadap dokumen resmi, publikasi akademik, laporan kebijakan, serta artikel yang membahas dinamika dan kesenjangan dalam implementasi kebijakan keamanan siber antarnegara anggota ASEAN.

1.8.6 Teknik Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan melalui metode studi kepustakaan *(library research),* dengan fokus pada isu implementasi kebijakan keamanan siber ASEAN. Peneliti mengakses berbagai sumber informasi yang

kredibel dan relevan, seperti jurnal ilmiah, dokumen kebijakan, laporan resmi ASEAN, buku, serta data dari situs web institusi terkait. Metode ini mencakup penelusuran informasi melalui media elektronik maupun non-elektronik guna memperoleh landasan teoritis dan data empiris yang mendukung analisis terhadap kesenjangan implementasi kebijakan keamanan siber di beberapa negara kawasan Asia Tenggara.

1.8.7 Analisis dan Interpretasi Data

Teknik analisis data dalam penelitian ini menggunakan pendekatan kualitatif. Analisis dilakukan dengan menelaah secara mendalam berbagai informasi terkait implementasi kebijakan keamanan siber ASEAN, yang kemudian dihubungkan dengan data lain untuk memperoleh pemahaman yang lebih utuh. Tujuannya adalah untuk mengidentifikasi pola, relasi, dan dinamika yang memengaruhi kesenjangan antarnegara anggota ASEAN dalam merespons ancaman siber, serta untuk memperkuat validitas temuan melalui triangulasi data yang relevan.

1.8.7.1 Reduksi Data

Proses reduksi data dalam penelitian ini dilakukan dengan menyaring dan menyederhanakan informasi agar hanya hal-hal pokok yang relevan dengan fokus studi yang dianalisis. Dalam konteks penelitian ini, data yang dikumpulkan akan difokuskan pada informasi mengenai dinamika implementasi kebijakan keamanan siber ASEAN, khususnya yang berkaitan dengan faktor-faktor yang menyebabkan terjadinya kesenjangan antarnegara anggota dalam menghadapi ancaman siber.

Data yang tidak relevan akan dieliminasi agar analisis lebih terarah dan mendalam.

1.8.7.2 Penyajian Data

Penyajian data dalam penelitian ini dilakukan dalam berbagai bentuk agar dapat diolah dan dipahami secara lebih jelas dan sistematis. Data akan disajikan dalam bentuk teks naratif, tabel, maupun bagan yang memuat informasi terkait implementasi kebijakan keamanan siber ASEAN, khususnya dalam menjelaskan kesenjangan antarnegara anggota dalam merespons ancaman siber. Penyajian ini bertujuan untuk menggambarkan dinamika, kepentingan strategis, dan konsistensi komitmen kolektif ASEAN dalam membangun keamanan digital kawasan secara efektif.

1.8.7.2 Pengambilan Kesimpulan

Data yang telah dihimpun dalam penelitian ini akan dianalisis menggunakan pendekatan matriks kepentingan nasional (national interest matrix) untuk menjawab rumusan masalah terkait kesenjangan implementasi kebijakan keamanan siber ASEAN. Melalui analisis ini, peneliti berupaya mengidentifikasi dan memahami kepentingan strategis masing-masing negara anggota ASEAN yang memengaruhi efektivitas dan konsistensi kerja sama regional dalam menghadapi ancaman siber pada tahun 2024.

1.8.8 Kualitas Data (*goodness criteria*)

Kualitas data dalam penelitian ini bersifat kualitatif dan berlandaskan pada paradigma konstruktivisme, di mana data diperoleh dan dianalisis berdasarkan

otentisitas dan kredibilitas informasi yang merefleksikan realitas implementasi kebijakan keamanan siber ASEAN. Penilaian dilakukan dengan memahami perspektif para aktor terkait, termasuk negara-negara anggota ASEAN, dalam menyikapi dinamika dan kesenjangan kerja sama keamanan siber regional tahun 2024.