BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi dalam dua dekade terakhir telah mendorong terjadinya transformasi besar dalam berbagai aspek kehidupan masyarakat global. Kemajuan teknologi digital tidak hanya mengubah cara individu berkomunikasi dan berinteraksi, tetapi juga mentransformasi mekanisme ekonomi, tata kelola pemerintahan, sistem pertahanan, hingga hubungan antarnegara dalam sistem internasional. Berbagai sektor strategis seperti perbankan, perdagangan, kesehatan, energi, transportasi, hingga administrasi pemerintahan saat ini telah terintegrasi dengan teknologi digital yang memungkinkan proses pertukaran informasi berlangsung secara cepat, efisien, dan lintas batas. Namun, transformasi tersebut juga menghasilkan bentuk-bentuk ancaman baru yang semakin kompleks. Lanskap keamanan internasional yang sebelumnya didominasi oleh ancaman konvensional secara perlahan mengalami pergeseran menuju ancaman non-tradisional yang berasal dari ruang siber, sehingga isu keamanan siber kini menjadi bagian integral dari agenda keamanan nasional dan internasional kontemporer (Morgan, 2020).

Urgensi persoalan tersebut semakin meningkat seiring dengan tingginya ketergantungan masyarakat global terhadap teknologi digital. The Global Risks Report menempatkan ancaman siber sebagai salah satu risiko global utama yang berpotensi mengganggu stabilitas ekonomi, keamanan nasional, serta keberlangsungan pelayanan publik di berbagai negara, dan risiko tersebut diperkirakan akan terus meningkat seiring perkembangan kecerdasan buatan, komputasi awan, dan Internet of Things (World Economic Forum, 2025).

Salah satu ancaman yang berkembang pesat dalam ruang siber adalah kejahatan siber (cyber crime), yang memiliki karakteristik jauh lebih sulit dicegah maupun ditangani oleh satu negara secara mandiri dibandingkan kriminalitas

konvensional. Karakteristik pertama adalah sifatnya yang transnasional: pelaku dapat menyerang dari suatu negara, menggunakan infrastruktur digital di negara lain, dan menargetkan korban di yurisdiksi berbeda, sehingga batas-batas geografis yang selama ini menjadi dasar sistem keamanan negara menjadi kabur (Caballero-Anthony, 2015). Karakteristik kedua adalah sifat anonim yang memungkinkan pelaku menyembunyikan identitas melalui VPN, proxy server, botnet, hingga enkripsi kompleks, sehingga proses atribusi memerlukan kerja sama internasional yang luas. Karakteristik ketiga adalah sifat asimetris: berbeda dari ancaman militer tradisional, serangan siber dapat dilakukan oleh individu atau kelompok kecil dengan sumber daya terbatas, namun berdampak besar terhadap institusi negara maupun layanan publik.

Karakteristik-karakteristik tersebut menunjukkan bahwa pendekatan keamanan yang bersifat unilateral atau self-help tidak lagi memadai untuk menghadapi ancaman siber kontemporer. Negara tidak dapat mengandalkan kemampuan domestiknya semata karena ancaman yang dihadapi bergerak melintasi yurisdiksi nasional dan melibatkan berbagai aktor internasional. Oleh karena itu, kerja sama internasional, khususnya dalam bentuk pertukaran informasi, koordinasi penanganan insiden, dan pembangunan kapasitas, menjadi kebutuhan yang tidak dapat dihindari dalam tata kelola keamanan siber modern (Caballero-Anthony, 2015).

Dalam konteks Asia Tenggara, tantangan tersebut menjadi semakin relevan karena kawasan ini merupakan salah satu pusat pertumbuhan ekonomi digital tercepat di dunia. Seiring meningkatnya digitalisasi, negara-negara ASEAN juga menghadapi risiko yang semakin besar terhadap berbagai bentuk kejahatan siber yang dapat mengganggu stabilitas kawasan, sehingga keamanan siber menjadi salah satu isu strategis dalam agenda kerja sama regional ASEAN.

Di antara negara-negara anggota ASEAN, Indonesia menempati posisi yang sangat penting dalam perkembangan ekonomi digital kawasan. Sebagai negara dengan jumlah penduduk terbesar di Asia Tenggara, Indonesia merupakan

kontributor terbesar terhadap nilai ekonomi digital ASEAN (Temasek et al., 2020), dengan jumlah pengguna internet yang telah mencapai lebih dari dua ratus juta orang (APJII, 2023). Besarnya skala transformasi digital tersebut di satu sisi membuka akses ekonomi yang lebih luas, namun di sisi lain juga meningkatkan kerentanan terhadap ancaman siber. Posisi Indonesia sebagai kekuatan ekonomi digital terbesar di kawasan secara bersamaan menjadikannya salah satu target utama berbagai bentuk serangan siber (Budiman, 2022).

Fenomena tersebut menggambarkan adanya cyber maturity gap, yaitu kesenjangan antara pesatnya pertumbuhan ekonomi digital dengan tingkat kematangan kapasitas keamanan siber suatu negara. Dalam konteks Indonesia, perkembangan ekonomi digital yang sangat cepat belum sepenuhnya diikuti oleh penguatan kapasitas pertahanan siber yang setara, sehingga berbagai institusi strategis nasional masih menghadapi risiko yang cukup tinggi terhadap ancaman siber yang terus berkembang, baik dari segi kuantitas maupun kompleksitas serangan (Budiman, 2022).

Indikasi adanya cyber maturity gap tersebut terlihat melalui berbagai insiden siber besar di Indonesia dalam beberapa tahun terakhir. Pada Januari 2022, kelompok ransomware Conti mengklaim berhasil memperoleh data sensitif yang berkaitan dengan Bank Indonesia (CNN, 2022). Pada Mei 2023, Bank Syariah Indonesia (BSI) menjadi korban serangan ransomware LockBit 3.0 yang mengganggu layanan perbankan dan mengekspos jutaan data nasabah (Komalasari, 2023). Kerentanan tersebut kembali terlihat pada Juni 2024 ketika Pusat Data Nasional (PDN) mengalami gangguan serius akibat serangan ransomware Brain Cipher, varian dari LockBit 3.0, yang melumpuhkan layanan lebih dari 200 instansi pemerintah dan mengungkap persoalan mendasar dalam tata kelola keamanan siber nasional, termasuk belum optimalnya sistem pencadangan data pemerintah (Tempo, 2024).

Tingginya tingkat ancaman siber terhadap Indonesia juga tercermin dari data yang dirilis pada paruh pertama tahun 2025, yaitu Badan Siber dan Sandi

Negara (BSSN) mendeteksi sekitar 3,64 miliar aktivitas serangan siber yang menargetkan berbagai sektor strategis nasional, meningkat tajam dari 330,5 juta anomali pada tahun 2024. Situasi ini diperkuat oleh sejumlah insiden besar yang menunjukkan bahwa kerentanan ini bukan sekadar potensi, melainkan kenyataan yang terus berulang, salah satunya dugaan kebocoran sekitar 279 juta data peserta BPJS Kesehatan pada 2021, yang mencakup data kependudukan hingga riwayat kesehatan (Nugraha et al., 2025). Rentetan insiden sejak 2021 hingga 2025 ini memperlihatkan pola yang relatif konsisten, yaitu berbagai sektor strategis (perbankan, data pribadi masyarakat, hingga infrastruktur digital pemerintah) terus menjadi sasaran, sehingga menunjukkan bahwa tantangan utama Indonesia bukan sekadar meningkatnya jumlah serangan, melainkan bagaimana membangun kapasitas ketahanan siber nasional yang mampu beradaptasi dengan ancaman yang berkembang sangat cepat.

Menghadapi eskalasi ancaman tersebut, Indonesia tidak memilih untuk mengandalkan pendekatan unilateral semata. Kompleksitas kejahatan siber yang bersifat lintas batas menyebabkan kemampuan domestik saja tidak pernah cukup untuk melakukan deteksi, atribusi, maupun penanganan insiden secara efektif, sehingga keterlibatan dalam kerja sama kawasan (regionalisme) menjadi pilihan yang rasional bagi negara-negara Asia Tenggara, termasuk Indonesia.

Salah satu wujud konkret kerja sama kawasan tersebut adalah ASEAN Cybersecurity Cooperation Strategy (ACCS). Setelah strategi pertama (2017 sampai 2020) yang berfokus pada penguatan kerja sama CERT-CERT dan pembangunan kapasitas, ASEAN menyusun ACCS periode 2021 sampai 2025 yang memperluas cakupan kerja sama ke dalam lima dimensi kerja (five dimensions of work): (1) Advancing Cyber Readiness Cooperation, (2) Strengthening Regional Cyber Policy Coordination, (3) Enhancing Trust in Cyberspace, (4) Regional Capacity Building, dan (5) International Cooperation (ASEAN, 2021).

ACCS dapat dipahami sebagai sebuah rezim kawasan (regional regime) di bidang keamanan siber (Krasner, 1982), yang diwujudkan melalui kelima dimensi

kerja tersebut. Namun, penting dicatat bahwa unsur norma dalam ACCS bukanlah norma yang dirumuskan secara orisinal oleh ASEAN, melainkan norma perilaku negara yang bertanggung jawab di ruang siber sebagaimana termuat dalam laporan UN Group of Governmental Experts (UNGGE) 2015, yang diadopsi ASEAN secara in-principle pada 2018 dan diterjemahkan menjadi satu inisiatif administratif di bawah Dimension 2, yaitu penyusunan Matrix/Regional Action Plan on the Implementation of Norms of Responsible State Behaviour in Cyberspace. Dengan demikian, ACCS tidak memuat seperangkat norma tersendiri yang dapat diuraikan secara mandiri dari teksnya sendiri, sebab norma tersebut bersifat derivatif dan hanya menjadi salah satu dari lima dimensi kerja ACCS, bukan fondasi konseptual keseluruhan strategi.

Dimensi yang justru dielaborasi paling konkret dan terukur dalam ACCS adalah Dimension 1: Advancing Cyber Readiness Cooperation, yang berfokus pada koordinasi CERT (Computer Emergency Response Team) serta pertukaran informasi ancaman (threat information sharing) antarnegara anggota, melalui inisiatif ASEAN Regional CERT Establishment dan ASEAN CERT Information Exchange Mechanism. Melalui mekanisme ini, negara-negara ASEAN dapat saling bertukar informasi mengenai pola serangan, indikator ancaman, serta praktik terbaik penanganan insiden secara lebih cepat, tanpa bergantung sepenuhnya pada kapasitas satu negara (ASEAN, 2021).

Bagi Indonesia, keterlibatan dalam mekanisme information sharing tersebut dapat ditelusuri setidaknya melalui tiga wujud konkret. Pertama, secara kelembagaan, melalui pembentukan Badan Siber dan Sandi Negara (BSSN) pada 2017 sebagai basis manajemen keamanan siber terpusat, serta keikutsertaan Indonesia dalam jejaring Computer Security Incident Response Team (CSIRT) yang terhubung dengan koordinasi ASEAN CERT di tingkat kawasan. Kedua, secara prosedural, melalui partisipasi dalam mekanisme koordinasi dan pertukaran informasi ancaman antar-CERT (CERT-to-CERT information exchange) yang menjadi inti dari ASEAN CERT Information Exchange Mechanism. Ketiga, melalui program pengembangan kapasitas sumber daya manusia, seperti

keikutsertaan dalam ASEAN Computer Incident Drill dan berbagai pelatihan penanganan insiden siber di tingkat kawasan.

Meskipun ketiga wujud keterlibatan tersebut telah berjalan, keterlibatan ini belum sepenuhnya berbanding lurus dengan penurunan ancaman siber domestik. Data yang telah dipaparkan sebelumnya justru menunjukkan pola sebaliknya, dengan volume anomali trafik siber yang melonjak tajam dan rangkaian insiden besar yang tetap berulang sepanjang periode yang sama. Kesenjangan antara keikutsertaan Indonesia dalam mekanisme information sharing ACCS (baik dari sisi kelembagaan, prosedural, maupun pengembangan kapasitas) dengan realitas ancaman siber domestik yang terus meningkat, inilah yang menjadi titik pijak persoalan penelitian ini.

Kesenjangan tersebut menimbulkan pertanyaan mendasar, bukan mengenai norma abstrak apa yang terkandung dalam ACCS (mengingat norma tersebut bersifat derivatif dari UNGGE dan tidak dielaborasi tersendiri dalam teks ACCS), melainkan mengenai bagaimana mekanisme konkret yang tersedia dalam rezim tersebut, khususnya pertukaran informasi melalui jaringan CERT pada Dimension 1, telah diimplementasikan di tingkat domestik Indonesia, dan sejauh mana implementasi tersebut berkontribusi terhadap upaya penanggulangan kejahatan siber nasional. Berdasarkan uraian tersebut, penelitian ini diajukan dengan judul: "IMPLEMENTASI MEKANISME PERTUKARAN INFORMASI (INFORMATION SHARING) DALAM SKEMA ASEAN CYBERSECURITY COOPERATION STRATEGY (ACCS) UNTUK MENANGGULANGI KEJAHATAN SIBER DI INDONESIA."

1.2 Pertanyaan Penelitian

Berdasarkan uraian yang telah disampaikan sebelumnya, maka peneliti merumuskan permasalahan penelitian dalam bentuk pertanyaan sebagai berikut:

1. Bagaimana kondisi kejahatan siber (cyber crime) yang dihadapi kawasan Asia Tenggara pada umumnya dan Indonesia pada khususnya sepanjang periode 2021 hingga 2025?
2. Bagaimana ASEAN Cybersecurity Cooperation Strategy (ACCS) dapat dipahami sebagai rezim kawasan (regional regime) keamanan siber, dilihat dari prinsip, norma, aturan, dan prosedur pengambilan keputusan yang terkandung di dalamnya?
3. Bagaimana implementasi mekanisme pertukaran informasi (information sharing) dalam skema ACCS oleh Indonesia, dan sejauh mana implementasi tersebut berkontribusi terhadap penanggulangan kejahatan siber domestik?

1.3 Ruang Lingkup dan Batasan Penelitian

Sebagaimana telah diuraikan pada sub-bab latar belakang, eskalasi insiden siber yang menimpa sektor perbankan, data pemerintahan, jaminan sosial, dan bank sentral Indonesia sepanjang 2021 hingga 2025 menegaskan bahwa persoalan kejahatan siber tidak dapat lagi dipandang sebagai persoalan teknis semata, melainkan sebagai persoalan yang menuntut respons kebijakan yang terarah pada level domestik maupun kawasan (Budiman, 2022). Untuk menjaga agar respons kebijakan tersebut dapat dianalisis secara mendalam tanpa kehilangan fokus, penelitian ini membatasi kajiannya pada tiga dimensi pokok, yaitu dimensi lokus, dimensi temporal, dan dimensi substansi, yang satu sama lain saling mengunci dan menopang argumentasi yang telah dibangun pada bagian latar belakang.

Secara lokus, penelitian ini memusatkan perhatian pada Indonesia sebagai unit analisis utama dalam konteks kawasan Asia Tenggara, mengingat Indonesia merupakan salah satu negara anggota ASEAN dengan eksposur ancaman siber yang relatif tinggi terhadap sektor-sektor strategis, sejalan dengan karakter kejahatan siber yang bersifat transnasional dan tidak mengenal batas yurisdiksi konvensional (Caballero-Anthony, 2015; D. S. Wall, 2007). Kawasan Asia Tenggara ditempatkan sebagai konteks eksternal yang melahirkan ASEAN Cybersecurity Cooperation

Strategy (ACCS) sebagai wujud regionalisme sektoral ASEAN di bidang keamanan siber (Acharya, 2001), namun analisis mendalam mengenai negara anggota ASEAN lainnya berada di luar cakupan penelitian ini, kecuali sejauh diperlukan untuk menjelaskan posisi dan peran Indonesia di dalam rezim kawasan tersebut.

Secara temporal, penelitian ini membatasi rentang pengamatan pada periode 2021 hingga 2025, dengan pertimbangan bahwa rentang waktu tersebut mencakup rangkaian insiden siber signifikan yang menimpa sektor kritis Indonesia, sebagaimana telah dipetakan pada latar belakang, sekaligus periode konsolidasi ACCS sebagai kerangka kerja sama kawasan pascadisahkannya sejumlah dokumen strategis ASEAN di bidang keamanan siber. Peristiwa maupun kebijakan yang berada di luar rentang tersebut tidak menjadi objek analisis utama, meskipun dapat disinggung secara terbatas sebagai konteks historis atau kecenderungan lanjutan apabila relevan untuk memperkuat argumentasi, tanpa mengubah batas waktu pokok penelitian.

Secara substansi, penelitian ini tidak bermaksud membedah keseluruhan lima dimensi kerja sama yang termuat di dalam ACCS, melainkan memfokuskan diri pada dua hal yang saling berkaitan. Pertama, ACCS dianalisis sebagai rezim kawasan yang memuat prinsip, norma, aturan, dan prosedur pengambilan keputusan sebagaimana kerangka rezim klasik (Krasner, 1982). Kedua, dari kelima dimensi kerja sama yang tercakup di dalam ACCS, penelitian ini memusatkan perhatian secara khusus pada mekanisme pertukaran informasi (information sharing) sebagai titik masuk analisis implementasi, karena mekanisme tersebut merupakan prasyarat operasional bagi keempat dimensi kerja sama lainnya sekaligus instrumen yang paling langsung bersinggungan dengan penanggulangan kejahatan siber domestik di Indonesia (Zrahia, 2018). Pembatasan ini diperlukan mengingat keterbatasan waktu dan sumber daya penelitian, serta untuk menjaga kedalaman analisis dibandingkan cakupan yang terlampau luas, sejalan dengan corak kualitatif-deskriptif yang telah ditetapkan sebagai pendekatan penelitian ini.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan sebelumnya, serta ruang lingkup yang telah ditetapkan pada sub-bab 1.3, penelitian ini disusun untuk mencapai tiga tujuan yang saling berkaitan secara berjenjang, bergerak dari pemetaan kondisi empiris di tingkat kawasan dan domestik, menuju analisis kelembagaan ACCS sebagai rezim, dan berakhir pada analisis implementasi yang menjadi inti persoalan penelitian.

Pertama, penelitian ini bertujuan untuk mendeskripsikan dan menganalisis kondisi kejahatan siber di kawasan Asia Tenggara pada umumnya dan di Indonesia pada khususnya, termasuk karakteristik, tren, serta eskalasi ancaman yang dihadapi sepanjang periode 2021 hingga 2025, sebagai landasan empiris yang memperkuat argumen pada latar belakang mengenai urgensi keterlibatan Indonesia dalam kerja sama kawasan.

Kedua, penelitian ini bertujuan untuk menganalisis ASEAN Cybersecurity Cooperation Strategy (ACCS) sebagai rezim kawasan keamanan siber, dengan mengidentifikasi prinsip, norma, aturan, dan prosedur pengambilan keputusan yang melekat di dalamnya (Krasner, 1982), sekaligus memetakan program dan mekanisme kerja sama yang tercakup di dalam kerangka tersebut sebagai dasar bagi analisis implementasi pada tujuan berikutnya.

Ketiga, penelitian ini bertujuan untuk menganalisis implementasi mekanisme pertukaran informasi (information sharing) dalam skema ACCS sebagai instrumen penanggulangan kejahatan siber domestik di Indonesia, termasuk sejauh mana mekanisme tersebut diserap dan dijalankan oleh Indonesia dalam merespons ancaman siber yang dihadapinya, sebagai jawaban konkret atas rumusan masalah ketiga sekaligus muara dari keseluruhan alur analisis penelitian ini.

1.5 Kerangka Konseptual

Kerangka konseptual dalam penelitian ini disusun secara deduktif, bergerak dari konsep yang paling umum menuju konsep yang paling spesifik dan operasional,

guna menyediakan alat analisis yang runtut bagi ketiga rumusan masalah penelitian sekaligus meneruskan alur argumentasi yang telah dibangun pada latar belakang mengenai posisi Indonesia sebagai aktor yang aktif menginternalisasi nilai dan norma kawasan. Alur ini dimulai dari konsep kerja sama kawasan sebagai landasan paling dasar mengenai mengapa negara-negara membentuk kerja sama sektoral di tingkat regional, dilanjutkan dengan konsep rezim kawasan yang menempatkan ACCS secara spesifik sebagai sebuah rezim, kemudian konsep keamanan siber dan kejahatan siber yang menjadi bingkai substantif persoalan, dan diakhiri dengan konsep mekanisme penanggulangan kejahatan siber yang memusatkan perhatian pada pertukaran informasi sebagai instrumen operasional utama.

1.5.1 Konsep Kerja Sama Kawasan (Regionalisme)

Konsep kerja sama kawasan, atau regionalisme, menjadi titik tolak paling mendasar untuk menjelaskan mengapa negara-negara di suatu kawasan geografis tertentu memilih untuk membentuk pengaturan kerja sama sektoral, termasuk di bidang keamanan siber. Secara umum, regionalisme dipahami sebagai proses pembentukan tatanan kerja sama antarnegara dalam suatu kawasan yang didorong oleh kesamaan kepentingan, saling ketergantungan fungsional, serta kebutuhan untuk mengelola persoalan bersama yang tidak dapat diselesaikan secara memadai melalui pendekatan unilateral (Acharya, 2001). Dalam konteks Asia Tenggara, regionalisme yang dibangun melalui ASEAN sejak awal telah menekankan prinsip konsensus, non-intervensi, serta penyelesaian persoalan bersama melalui dialog dan pembentukan norma secara bertahap, alih-alih melalui pembentukan institusi supranasional yang mengikat secara ketat, sebuah pola yang oleh Acharya (2001) disebut sebagai proses konstruksi komunitas keamanan yang bertumpu pada interaksi diplomatik berulang alih-alih pada instrumen hukum formal yang kaku.

Kerja sama sektoral kawasan, termasuk di bidang keamanan siber, pada dasarnya merupakan kelanjutan logis dari watak regionalisme tersebut. Ketika suatu persoalan, seperti kejahatan siber, memiliki karakter lintas batas yang tidak dapat ditangani secara efektif oleh satu negara saja, kawasan menjadi skala pengelolaan yang paling rasional sebelum bergerak ke tingkat kerja sama global

yang lebih kompleks dan lambat mencapai konsensus (Caballero-Anthony, 2015). Pembentukan kerja sama sektoral di tingkat kawasan memungkinkan negara-negara anggota untuk menyelaraskan kepentingan nasional mereka dengan kepentingan kolektif kawasan melalui proses interaksi yang berulang, sehingga secara bertahap melahirkan pengaturan bersama mengenai bagaimana suatu persoalan seharusnya dikelola (Acharya, 2003). Pengaturan bersama inilah yang kemudian mengkristal ke dalam bentuk kerja sama yang lebih terlembagakan, sebagaimana akan diuraikan pada sub-bab berikutnya melalui konsep rezim kawasan. Atas dasar itulah, pembentukan ASEAN Cybersecurity Cooperation Strategy (ACCS) dapat dipahami sebagai manifestasi konkret dari watak regionalisme ASEAN dalam merespons persoalan keamanan siber sebagai kepentingan bersama kawasan, sekaligus menjadi pijakan awal bagi penelitian ini sebelum bergerak menganalisis ACCS secara lebih spesifik sebagai sebuah rezim kawasan pada sub-bab berikutnya.

1.5.2 Konsep Rezim Kawasan (Regional Regime) dan ACCS sebagai Rezim Kawasan

Untuk membedah ACCS secara lebih spesifik dari sekadar wujud regionalisme yang bersifat umum, penelitian ini menggunakan konsep rezim internasional sebagaimana dirumuskan oleh Krasner (1982), yang mendefinisikan rezim sebagai seperangkat prinsip, norma, aturan, dan prosedur pengambilan keputusan implisit maupun eksplisit yang menjadi titik temu harapan aktor-aktor dalam suatu bidang hubungan internasional tertentu. Dalam definisi tersebut, prinsip merujuk pada keyakinan dasar mengenai fakta, sebab-akibat, dan kejujuran yang dianut bersama; norma merujuk pada standar perilaku yang dirumuskan dalam bentuk hak dan kewajiban; aturan merujuk pada ketentuan atau larangan spesifik bagi tindakan; sementara prosedur pengambilan keputusan merujuk pada praktik yang berlaku untuk membuat dan melaksanakan pilihan kolektif (Krasner, 1982). Definisi ini telah menjadi rujukan baku dalam kajian rezim internasional selama lebih dari empat dekade, dan tetap relevan digunakan untuk membedah kerja sama

sektoral kawasan yang bersifat lebih teknis, seperti keamanan siber, sekalipun awalnya dirumuskan dalam konteks isu-isu ekonomi-politik global.

Berpijak dari kerangka tersebut, penelitian ini mendudukkan ACCS bukan sekadar sebagai dokumen strategi teknis, melainkan sebagai sebuah rezim kawasan yang secara inheren memuat keempat unsur di atas. Sebagai rezim, ACCS memiliki prinsip dasar berupa keyakinan bersama bahwa keamanan siber merupakan tanggung jawab kolektif kawasan yang tidak dapat dipenuhi secara memadai melalui pendekatan unilateral negara anggota, sejalan dengan logika kalkulasi rasional yang telah diuraikan melalui Institusionalisme Liberal pada latar belakang penelitian. ACCS juga memuat norma berupa standar perilaku yang diharapkan dari negara anggota, termasuk komitmen terhadap keterbukaan informasi dan kesediaan berkoordinasi dalam penanganan insiden siber lintas batas. Selain itu, ACCS memuat aturan operasional yang lebih spesifik mengenai bentuk-bentuk kerja sama yang harus dijalankan, serta prosedur pengambilan keputusan yang mengatur mekanisme koordinasi antarnegara anggota, termasuk melalui forum-forum sektoral ASEAN di bidang keamanan siber (Krasner, 1982).

1.5.3 Konsep Keamanan Siber (Cybersecurity) dan Kejahatan Siber (Cybercrime)

Untuk keperluan analisis data empiris pada bab pembahasan, penelitian ini memerlukan definisi kerja yang jelas atas dua istilah kunci, yaitu keamanan siber dan kejahatan siber, sebelum keduanya dikaitkan dengan mekanisme penanggulangan yang menjadi fokus akhir kerangka konseptual ini. Keamanan siber, dalam penelitian ini, dipahami sebagai kondisi terlindunginya sistem, jaringan, data, dan infrastruktur digital suatu negara dari ancaman, gangguan, maupun serangan yang dapat mengancam kerahasiaan, integritas, dan ketersediaan informasi, sekaligus mencakup keseluruhan upaya kebijakan, kelembagaan, dan teknis yang ditempuh untuk mencapai kondisi tersebut. Definisi ini menempatkan keamanan siber tidak semata sebagai persoalan teknis pertahanan sistem, melainkan juga sebagai persoalan kebijakan dan tata kelola yang melibatkan negara, sektor

swasta, dan kerja sama internasional, sejalan dengan argumen bahwa ancaman siber terhadap sektor kritis telah berkembang menjadi tantangan strategis yang membahayakan kepentingan nasional (Budiman, 2022).

Adapun kejahatan siber dipahami sebagai setiap tindakan melawan hukum yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi sebagai sarana, sasaran, maupun keduanya. Wall (2007) menegaskan bahwa kejahatan siber berbeda secara mendasar dari kejahatan konvensional karena berlangsung di ruang jaringan yang tidak memiliki batas fisik yang jelas, sehingga menuntut kerangka penanganan yang juga berbeda dari pendekatan kepolisian tradisional. Karakteristik virtual, transnasional, anonim, dan asimetris yang melekat pada kejahatan siber (Caballero-Anthony, 2015; Habibi & Liviani, 2020) semakin diperkuat oleh klasifikasi (D. Wall, 2003) yang membedakan ragam kejahatan siber ke dalam beberapa kategori, mulai dari pelanggaran akses sistem hingga penipuan dan pencurian data, sebuah keragaman bentuk yang tercermin pula pada kasus-kasus yang menimpa Indonesia. Kejahatan siber dalam penelitian ini mencakup, namun tidak terbatas pada, serangan ransomware, kebocoran data, serta gangguan operasional terhadap sistem elektronik sektor strategis, sebagaimana ditemukan pada sejumlah insiden yang menimpa sektor perbankan, data pemerintahan, jaminan sosial, dan bank sentral Indonesia sepanjang periode 2021 hingga 2025. Kedua definisi kerja ini akan menjadi rujukan konsisten dalam membedah data empiris pada Bab IV, khususnya dalam menjelaskan kondisi kejahatan siber di Indonesia dan Asia Tenggara sebagaimana dimaksud pada rumusan masalah pertama.

1.5.4 Konsep Mekanisme Penanggulangan Kejahatan Siber

Setelah menetapkan definisi kerja atas keamanan siber dan kejahatan siber pada sub-bab sebelumnya, sub-bab ini bergerak pada tataran yang lebih operasional, yaitu bagaimana ancaman tersebut ditanggulangi melalui kerja sama kawasan. Secara umum, penanggulangan kejahatan siber di tingkat kawasan dapat ditempuh melalui berbagai mekanisme kerja sama, antara lain harmonisasi regulasi lintas

negara, peningkatan kapasitas kelembagaan melalui pelatihan dan pengembangan sumber daya manusia, penyusunan kerangka hukum acara bersama untuk penanganan bukti digital lintas yurisdiksi, latihan simulasi keamanan siber bersama, serta pertukaran informasi mengenai pola serangan, kerentanan, dan ancaman yang sedang berkembang (Zrahia, 2018). Kelima mekanisme tersebut pada dasarnya saling melengkapi dan tercakup di dalam berbagai dimensi kerja sama yang termuat di dalam ACCS sebagaimana telah diuraikan pada sub-bab 1.5.2.

Di antara berbagai mekanisme tersebut, penelitian ini secara khusus memusatkan perhatian pada mekanisme pertukaran informasi (information sharing), sejalan dengan arahan yang menegaskan bahwa dari keseluruhan mekanisme yang tercakup di dalam kerja sama keamanan siber kawasan, terdapat satu poin krusial yang menjadi prasyarat bagi efektivitas mekanisme lainnya, yaitu pertukaran informasi. Dalam literatur keamanan siber, pertukaran intelijen ancaman dipandang sebagai strategi pertahanan mutakhir yang memungkinkan satu organisasi atau negara mengubah kemampuan deteksinya menjadi kemampuan pencegahan bagi pihak lain, sehingga mengurangi duplikasi upaya di antara para pihak yang saling terhubung (Zrahia, 2018). Riset terbaru turut menegaskan bahwa sifat intelijen ancaman siber, yang memadukan data teknis mentah dengan pemahaman kontekstual manusia, membuat pertukaran informasi ini berbeda dari bentuk-bentuk pertukaran data pada umumnya dan menuntut kepercayaan serta kerangka kelembagaan tersendiri agar dapat berjalan efektif lintas yurisdiksi (Abraham et al., 2025).

Mekanisme ini dipilih sebagai fokus analisis karena tiga alasan. Pertama, pertukaran informasi merupakan prasyarat operasional yang mendasari mekanisme-mekanisme lain; tanpa akses terhadap informasi mengenai pola serangan dan kerentanan terkini dari negara mitra, upaya harmonisasi regulasi maupun penguatan kapasitas kelembagaan akan berjalan tanpa basis data yang memadai (Abraham et al., 2025). Kedua, pertukaran informasi merupakan dimensi kerja sama yang paling langsung bersinggungan dengan kebutuhan operasional Indonesia dalam mendeteksi dan merespons insiden siber secara cepat,

sebagaimana tercermin dalam keterlibatan Indonesia pada jaringan CERT regional yang telah disinggung pada latar belakang penelitian. Ketiga, mekanisme ini menyediakan indikator yang relatif dapat diamati dan ditelusuri jejaknya secara empiris, baik melalui kebijakan domestik maupun praktik kelembagaan Indonesia, sehingga memungkinkan penelitian ini untuk menjawab rumusan masalah ketiga secara lebih terarah dibandingkan apabila seluruh dimensi ACCS dianalisis secara sekaligus. Dengan demikian, konsep mekanisme pertukaran informasi ini menjadi titik tumpu operasional yang menghubungkan kerangka rezim ACCS pada sub-bab 1.5.2 dengan analisis empiris implementasinya di Indonesia pada Bab IV, sekaligus menutup alur deduktif kerangka konseptual yang dibangun sejak konsep regionalisme pada sub-bab 1.5.1.

1.6 Asumsi Peneliti

Sebagai penelitian kualitatif dengan sifat deskriptif analitis, penelitian ini tidak menempatkan asumsi sebagai hipotesis yang hendak diuji secara statistik, melainkan sebagai proposisi dasar yang diturunkan secara deduktif dari kerangka konseptual pada sub-bab 1.5 dan kerangka analisis pada sub-bab 1.7. Asumsi ini berfungsi sebagai titik pijak berpikir yang memandu arah pembacaan data pada Bab IV, sekaligus menjaga konsistensi antara premis konseptual yang telah dibangun dengan cara peneliti menafsirkan temuan empiris di lapangan. Peneliti berasumsi bahwa peningkatan skala dan kompleksitas kejahatan siber di Indonesia, sebagaimana ditunjukkan oleh data BSSN dan rangkaian insiden besar sepanjang 2021 hingga 2025, tidak dapat lagi ditangani secara memadai melalui kapasitas domestik semata. Sifat kejahatan siber yang transnasional, anonim, dan asimetris menjadikan kerja sama kawasan sebagai kebutuhan struktural, bukan sekadar pilihan kebijakan, sehingga keterlibatan Indonesia dalam ACCS beralasan untuk dipahami sebagai respons yang rasional terhadap kondisi ancaman yang terus meningkat.

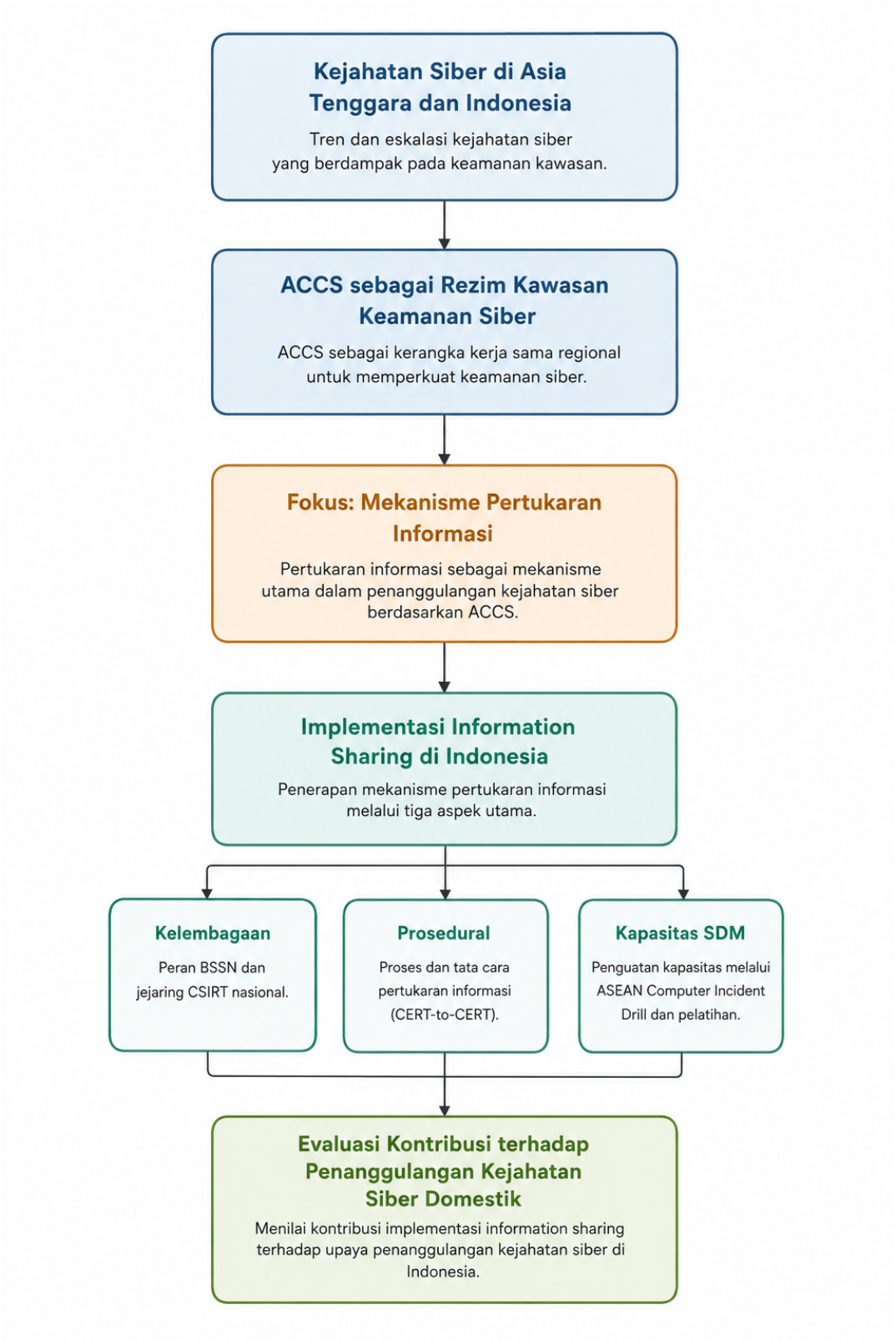
Bertolak dari premis tersebut, peneliti berasumsi bahwa ACCS, sebagai rezim kawasan yang bersifat non-mengikat secara hukum, tetap memiliki daya

pengaruh terhadap perilaku negara anggota, termasuk Indonesia, bukan melalui kepatuhan formal terhadap seperangkat norma tertentu, melainkan melalui ketersediaan dan pemanfaatan mekanisme kerja sama operasional yang konkret di dalamnya. Asumsi ini konsisten dengan temuan pada sub-bab 1.5.2 bahwa norma dalam ACCS bersifat derivatif dari UN Group of Governmental Experts 2015 dan tidak dielaborasi tersendiri dalam teks ACCS, sehingga daya ikat ACCS terhadap Indonesia lebih tepat dipahami melalui keberfungsian mekanismenya. Sejalan dengan itu, peneliti juga berasumsi bahwa partisipasi Indonesia dalam mekanisme pertukaran informasi ACCS didorong oleh kebutuhan praktis untuk mengatasi keterbatasan kapasitas domestik dalam mendeteksi, mengatribusi, dan merespons ancaman siber lintas batas, alih-alih oleh proses internalisasi norma secara sosiologis. Dengan kata lain, keikutsertaan Indonesia dipandang sebagai kalkulasi kepentingan nasional dalam menghadapi keterbatasan sumber daya dan informasi yang tidak dapat dipenuhi secara sepihak, sejalan dengan logika kerja sama kawasan yang telah diuraikan pada sub-bab 1.5.1, tanpa perlu menempatkan proses tersebut ke dalam bingkai pembentukan identitas maupun kesepahaman bersama yang bersifat sosiologis.

Terakhir, peneliti berasumsi bahwa tingkat implementasi mekanisme pertukaran informasi ACCS di Indonesia dapat ditelusuri dan dinilai secara empiris melalui tiga indikator yang saling melengkapi, yaitu kelembagaan yang dibentuk, prosedur kerja sama yang benar-benar dijalankan, dan program pengembangan kapasitas yang diikuti. Ketiga indikator tersebut diasumsikan sebagai representasi yang memadai untuk menilai sejauh mana Indonesia telah menyerap mekanisme kawasan ke dalam praktik domestiknya, sekaligus menjadi dasar untuk mengevaluasi kontribusi implementasi tersebut terhadap penanggulangan kejahatan siber nasional, sebagaimana telah dipetakan pada kerangka analisis di sub-bab 1.7. Rangkaian asumsi tersebut secara keseluruhan menegaskan posisi penelitian yang konsisten sejak sub-bab latar belakang hingga kerangka analisis, yaitu bahwa jawaban atas persoalan penelitian ini terletak pada penelusuran mekanisme dan implementasi yang dapat diverifikasi secara empiris.

1.7 Kerangka Analisis

Kerangka analisis penelitian ini disusun untuk menggambarkan alur berpikir yang menghubungkan kerangka konseptual pada sub-bab 1.5 dengan tahapan analisis pada Bab IV, sehingga setiap pertanyaan penelitian memiliki pijakan konseptual yang jelas dan setiap konsep memiliki tempat pendaratan yang jelas pula dalam pembahasan. Alur ini bergerak secara deduktif dari tataran empiris paling umum menuju tataran implementatif paling spesifik, mengikuti susunan pertanyaan penelitian yang telah dirumuskan pada sub-bab 1.2, sebagaimana divisualisasikan pada gambar berikut.



Gambar 1. Kerangka Analitis

Sebagaimana ditunjukkan pada gambar di atas, alur analisis dimulai dari pemetaan kondisi kejahatan siber di Asia Tenggara dan Indonesia sebagai basis empiris, kemudian bergerak menuju pembahasan ACCS sebagai rezim kawasan yang secara inheren memuat prinsip, norma, aturan, dan prosedur pengambilan keputusan. Dari titik itu, penelitian mempersempit fokus pada satu mekanisme kerja sama yang paling operasional, yaitu pertukaran informasi, sebelum akhirnya diuraikan ke dalam tiga wujud implementasi yang saling melengkapi di tingkat domestik Indonesia, yakni kelembagaan, prosedural, dan pengembangan kapasitas sumber daya manusia. Ketiga wujud tersebut kemudian dipertemukan kembali pada tahap akhir berupa evaluasi, yaitu membandingkan tingkat implementasi yang telah diuraikan dengan tren data ancaman siber yang telah dipetakan pada tahap pertama.

Dengan alur tersebut, kerangka analisis ini menegaskan bahwa penelitian tidak memperlakukan norma sebagai variabel yang harus dibuktikan keberadaannya secara terbuka, melainkan sebagai salah satu unsur bawaan dari status ACCS sebagai rezim kawasan yang telah ditetapkan sejak sub-bab 1.5.2. Seluruh energi analisis pada Bab IV dengan demikian dapat diarahkan sepenuhnya pada pertanyaan yang dapat dijawab secara empiris, yaitu bagaimana mekanisme pertukaran informasi tersebut diimplementasikan di Indonesia dan sejauh mana implementasinya berkontribusi terhadap penanggulangan kejahatan siber domestik, sehingga setiap tahap dalam kerangka ini bermuara secara runtut pada jawaban atas tiga pertanyaan penelitian yang telah dirumuskan pada sub-bab 1.2.