

BAB I

PENDAHULUAN

1.1 Latar Belakang Penelitian

Hubungan Internasional sebagai ilmu berangkat dari satu keadaan yang belum pernah berubah sejak sistem negara-negara terbentuk: dunia tidak memiliki pemerintah yang mengatur semuanya, sehingga negara-negara yang berbeda kepentingan, kapasitas, dan pandangan itu harus menata hubungannya sendiri. Ilmu ini lalu mempersoalkan tiga hal sekaligus, yaitu bagaimana konflik antarnegara dapat dicegah, bagaimana kerja sama dapat dijaga agar tetap berjalan, dan bagaimana persoalan yang melampaui satu negara dapat ditangani bersama tanpa mengorbankan kedaulatan masing-masing. Permasalahan yang diangkat dalam penelitian ini terletak pada persoalan ketiganya sekaligus. Kejahatan siber di Asia Tenggara melibatkan pelaku yang berbasis di satu negara, korban yang tersebar di negara lain, dana yang berpindah melalui kanal yang tidak mengenal perbatasan, dan negara-negara yang harus menentukan sendiri sejauh mana mereka mau membatasi kedaulatannya demi respons bersama. Dengan kata lain, persoalan yang tampaknya teknis itu pada dasarnya adalah persoalan klasik Hubungan Internasional mengenai kerja sama di tengah ketiadaan otoritas pusat.

Persoalan tersebut semakin layak dibaca sebagai persoalan keamanan setelah ilmu keamanan sendiri melebarkan cakupannya. Pandangan tradisional memandang keamanan sebagai upaya mempertahankan wilayah dan penduduk dari serangan militer, sehingga kejahatan yang tidak melibatkan senjata diletakkan di luar ranah keamanan dan ditangani oleh kepolisian masing-masing negara. Kerangka analitis yang dikembangkan Barry Buzan, Ole Wæver, dan Jaap de Wilde menolak batasan itu. Bagi mereka, keamanan tidak melekat pada suatu ancaman secara objektif, melainkan terbentuk ketika aktor tertentu berhasil meyakinkan audiens bahwa isu tersebut mengancam keberadaan sesuatu yang dianggap penting, lalu menuntut tindakan di luar prosedur politik biasa (Buzan et al., 1998). Kerangka ini menjelaskan mengapa kejahatan siber yang semula dianggap urusan teknis dapat berpindah kedudukan menjadi persoalan keamanan kawasan, dan mengapa perpindahan itu sendiri perlu dijelaskan daripada dianggap sebagai hal yang sudah jelas. Lebih jauh, pergeseran ini juga menempatkan negara-negara di dalam satu kawasan pada posisi yang saling tergantung: keamanan suatu negara ikut ditentukan oleh apa yang terjadi

di negara tetangganya, sehingga klaster geografis yang terbentuk tidak lagi dapat ditangani secara mandiri (Buzan & Wæver, 2003).

Kawasan Asia Tenggara menjadi ruang di mana persoalan itu terbentuk dengan karakteristiknya sendiri. Association of Southeast Asian Nations menyatukan sepuluh negara dengan tingkat kapasitas yang timpang, mulai dari negara dengan infrastruktur siber maju hingga negara yang kesiapannya masih jauh tertinggal. Asosiasi ini menata kerja sama atas dasar penghormatan terhadap kedaulatan, pengambilan keputusan secara konsensus, dan tidak campur tangan terhadap urusan dalam negeri negara anggota. Prinsip terakhir itu memiliki dua wajah pada saat yang sama. Di satu sisi ia menjaga keutuhan organisasi, sebab tidak ada negara yang merasa kedaulatannya akan diganggu oleh keputusan bersama. Di sisi lain ia membatasi bentuk respons yang dapat diambil, sebab tidak tersedia mekanisme yang dapat memaksa satu negara agar mengubah kebijakannya (ASEAN Secretariat, 1999; Krasner, 1983). Kondisi inilah yang menjadikan ASEAN objek kajian yang menarik bagi Hubungan Internasional: sebuah organisasi regional yang berpegang pada prinsip kedaulatan dan konsensus, namun diminta menangani persoalan yang sifatnya justru melintasi batas kedaulatan itu sendiri.

Dengan kerangka keilmuan dan kerangka keamanan tersebut sebagai pijakan, penelitian ini kemudian masuk ke persoalan yang sedang berkembang di lapangan, yaitu perkembangan teknologi informasi dan komunikasi yang mengubah tatanan keamanan global. Teknologi informasi dan komunikasi berkembang begitu cepat sepanjang abad ke-21, dan perkembangan itu mengubah tatanan keamanan global secara mendasar. Digitalisasi memang mendorong pertumbuhan ekonomi serta mempererat konektivitas antarnegara, tetapi di balik itu ia juga melahirkan ancaman baru yang melintasi batas negara dan sulit dijangkau mekanisme keamanan konvensional. Kejahatan siber (*cybercrime*) beserta berbagai bentuk kejahatan transnasional yang memakai infrastruktur digital sebagai medium operasionalnya merupakan wujud paling nyata dari ancaman tersebut (Sari, 2024).

Kawasan Asia Tenggara, yang dihimpun dalam wadah *Association of Southeast Asian Nations* (ASEAN), tidak luput dari dinamika tersebut. Ekonomi ASEAN pada 2022 tercatat melampaui 3,6 triliun dolar Amerika Serikat, angka yang menempatkannya sebagai ekonomi terbesar kelima di dunia (ASEANstats, 2024; S&P Global, 2024), dan pertumbuhan sebesar ini berjalan seiring dengan penetrasi internet serta adopsi teknologi digital yang terus naik di seluruh negara anggotanya. Sayangnya kemajuan digital itu justru membuat kawasan ini incaran utama kejahatan siber: penipuan daring, kebocoran data, sampai serangan terhadap infrastruktur kritis negara (INTERPOL, 2021).

Asia Tenggara adalah kawasan yang sangat terdigitalisasi dan berada di lokasi geostrategis. penetrasi internet kawasan ini mencapai 80% pada 2022, sementara ekonomi digitalnya menembus 100 miliar dolar AS setahun berselang. Digitalisasi yang melaju kencang, ditambah ketegangan geopolitik yang tak kunjung reda, membuat kejahatan siber berubah dari sekadar isu teknis menjadi ancaman mendesak kawasan ini kejahatan siber di Asia Tenggara melonjak 82% hanya dalam rentang 2021 ke 2022. Singapura, Indonesia, Thailand, dan Vietnam paling sering menjadi sasaran pada 2023, keempatnya juga negara dengan tingkat digitalisasi tertinggi di kawasan, sehingga lebih menggiurkan bagi pelaku kejahatan siber (Julia Brock, 2024).

Sebagian peretas yang beroperasi di kawasan ini punya keterkaitan dengan Tiongkok. Wired melaporkan serangan siber bernuansa Tiongkok terhadap negara-negara Asia Tenggara naik 20% setiap tahunnya, dan sejak 2019 peretas yang terhubung dengan pemerintah Tiongkok tercatat menembus server pemerintahan sejumlah negara kawasan ini untuk memata-matai serta mencuri email-email sensitif.

INTERPOL mencatat ancaman siber di Asia Pasifik naik tajam dalam beberapa tahun terakhir. Modus seperti *Crimeware-as-a-Service* (CaaS), penipuan siber, dan *cryptojacking* terus bermunculan, memanfaatkan celah pada negara-negara yang kapasitas pertahanan sibernya timpang satu sama lain (INTERPOL, 2021). Yang lebih mengkhawatirkan, munculnya pusat penipuan daring terorganisir tempat korban dipaksa bekerja seperti yang terjadi di Kamboja, Laos, dan Myanmar menunjukkan bahwa kejahatan siber sudah berevolusi menjadi kejahatan transnasional terorganisir dengan jaringan yang tidak sederhana (United Nations Office on Drugs and Crime [UNODC], 2023; Huang, 2024).

Di ASEAN, Myanmar dan Laos merupakan salah satu pusat kejahatan siber, dan alasannya adalah kedua negara sudah cukup lama terdampak konflik, secara umum wilayah yang terdampak konflik sering kali menjadi tempat berlindung bagi kejahatan terorganisasi lintas negara, peran sentral aktor negara dalam hal ini jarang mendapat perhatian. Di wilayah-wilayah tersebut, jaringan kriminal dapat beroperasi tanpa tersentuh hukum, serta kerap kali turut menopang konflik dan ekonomi subsisten. Kelompok-kelompok ini memanfaatkan celah penegakan hukum dan pola kendali wilayah yang rumit untuk mengambil keuntungan dari situasi kekacauan yang terjadi. (Australian Strategic Policy Institute, 8 September 2025)

Myanmar telah menjadi salah satu pusat kejahatan siber (*cybercrime*) dan kejahatan terorganisir transnasional terbesar di dunia. Kejahatan tersebut berpusat di wilayah

perbatasan seperti Myawaddy, sindikat internasional menjalankan mega-industri ilegal bernilai miliaran dolar, termasuk penipuan daring (*scamming*), judi online, dan pencucian uang, yang sering kali didorong oleh praktik perdagangan manusia dan pengekangan. Menurut Justice For Myanmar, operasi bisnis transnational crime ini dikendalikan oleh jaringan mafia berasal dari Tiongkok yang bekerja sama dengan Karen Border Guard Force (Karen National Army, KNA). (Tenri dan Atman, 2025)

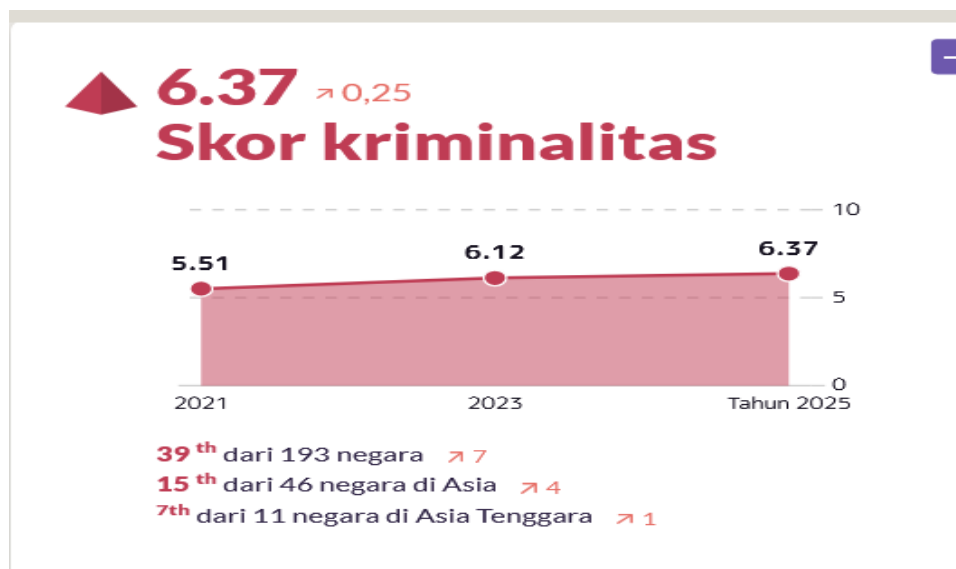
Gambar 1.1 Myanmar Criminal Score



Sumber: Global Initiative against Transnational Organized Crime (GI-TOC)

Sementara Laos, meskipun akses internet dan infrastruktur yang terbatas dapat mengurangi beberapa eksposur, Laos menghadapi kerentanan yang tumbuh dalam lanskap digitalnya, terutama dalam hal keterjangkauan, kualitas konektivitas, dan kesenjangan peraturan. Tantangan-tantangan ini tidak menghentikan munculnya ancaman cyber, yang tetap menjadi perhatian signifikan. Berbagai aktor terlibat, termasuk jaringan kriminal, warga negara dalam dan luar negeri, dan entitas sektor swasta. Pelaku sering mengeksploitasi platform media sosial populer untuk memikat korban ke dalam skema perdagangan cryptocurrency yang curang. (Global Organized Crime Index, diakses 2026).

Gambar 1.2 Skor Kriminalitas Laos



Sumber: Global Organized Crime Index, diakses 2026

Kedua negara dan juga negara-negara anggota ASEAN lainnya, telah melakukan upaya penanganan yang dilakukan oleh negara masing-masing. Namun dalam menghadapi ancaman yang bersifat lintas batas tersebut, respons tunggal oleh negara-bangsa terbukti tidak memadai. Sifat kejahatan siber yang memanfaatkan yurisdiksi berganda, anonimitas digital, dan kecepatan transaksi lintas negara menuntut pendekatan kolaboratif di tingkat regional maupun internasional (Nguyen et al., 2024).

Kondisi inilah yang membuat peran organisasi internasional, khususnya ASEAN, layak dikaji secara akademis. Kesenjangan kapasitas siber antarnegara anggota masih terasa nyata: Singapura dan Malaysia memiliki infrastruktur jauh lebih maju dibandingkan Laos atau Myanmar, dan kesenjangan itu membuat implementasi kebijakan tidak merata. ASEAN, yang berdiri sejak 1967, akhirnya mengambil inisiatif dan menyepakati komitmen penanganan kejahatan transnasional di tingkat regional, komitmen yang lantas diwujudkan lewat berbagai mekanisme kelembagaan.

Pada tahun 1999, ASEAN membentuk *Senior Officials Meeting on Transnational Crime* (SOMTC) sebagai wadah koordinasi kebijakan antarnegara anggota dalam memerangi kejahatan lintas batas (ASEAN Secretariat, 1999; Nguyen et al., 2024). Secara khusus, isu siber mulai dimasukkan sebagai salah satu dari sepuluh area kerja sama SOMTC sejak tahun 2001, dan pada tahun 2013 ASEAN membentuk *SOMTC Working Group on Cybercrime* (ASEAN, t.t.). Puncaknya, pada tahun 2017 ASEAN mengadopsi Deklarasi Pencegahan dan Penanggulangan Kejahatan Siber (ASEAN Secretariat, 2017b), dan pada tahun 2022 ASEAN menyepakati pembentukan *ASEAN Regional Computer*

Emergency Response Team (CERT) sebagai badan operasional regional di bidang keamanan siber (Cyber Security Agency of Singapore [CSA], 2022).

Serangkaian inisiatif tersebut mencerminkan transformasi pola tindak ASEAN dari sekadar forum dialog menjadi aktor kelembagaan yang memiliki peran normatif dan operasional. Namun demikian, sejumlah tantangan struktural tetap melingkupi efektivitas ASEAN dalam menangani *cybersecurity*. Prinsip non-intervensi dan konsensus yang menjadi pilar *ASEAN Way* acap kali menghambat pengambilan keputusan yang cepat dan mengikat (Alviyani et al., 2022). Kesenjangan kapasitas siber antarnegara anggota di mana Singapura dan Malaysia memiliki infrastruktur yang jauh lebih maju dibandingkan Laos atau Myanmar menciptakan ketidakmerataan dalam implementasi kebijakan bersama (Dobberstein et al., 2018; IISS, 2023). Selain itu, ketiadaan instrumen hukum yang mengikat di tingkat regional menjadikan kerja sama siber ASEAN lebih bergantung pada itikad baik negara anggota daripada kewajiban hukum formal (Huang, 2024).

Dalam kerangka teoritis Hubungan Internasional, persoalan ini relevan dikaji melalui beberapa lensa analitis. *Pertama*, *Neoliberal Institutionalism* yang dikembangkan oleh Robert O. Keohane memberikan dasar argumentasi bahwa organisasi internasional mampu mendorong kerja sama negara-negara yang saling bergantung dalam kondisi anarki internasional (Keohane, 1984). *Kedua*, *Regime Theory* yang diperkenalkan oleh Stephen Krasner membantu menjelaskan bagaimana ASEAN berfungsi sebagai rezim internasional yang menetapkan prinsip, norma, aturan, dan prosedur pengambilan keputusan di bidang keamanan siber (Krasner, 1983). *Ketiga*, *Securitization Theory* dari Mazhab Kopenhagen yang dikembangkan Barry Buzan, Ole Wæver, dan Jaap de Wilde memungkinkan analisis tentang bagaimana isu *cybercrime* dikonstruksikan sebagai ancaman eksistensial yang kemudian dipindahkan dari ranah politik biasa ke ranah keamanan (Buzan et al., 1998). Dan *Keempat*, *Regional Security Complex Theory* (RSCT) dari Barry Buzan dan Ole Wæver, yang menjelaskan bahwa masalah keamanan suatu negara sangat terikat dengan negara tetangga, menciptakan klaster geografis di mana ancaman tidak bisa ditangani secara mandiri.

Dimensi kajian ini merentang antara *low politics* di mana *cybercrime* dan kejahatan transnasional secara tradisional dikategorikan sebagai isu non-militer yang bersifat teknis dan fungsional hingga *high politics*, mengingat serangan siber terhadap infrastruktur kritis negara dapat berimplikasi langsung pada kedaulatan dan keamanan nasional (Buzan et al., 1998; Keohane & Nye, 1977). Persimpangan antara kedua dimensi inilah yang menjadikan

ASEAN sebagai laboratorium kajian yang menarik: sejauh mana sebuah organisasi regional yang berpegang pada prinsip kedaulatan dan konsensus mampu menjalankan fungsi tata kelola keamanan siber yang efektif.

Pemilihan studi kasus Myanmar dan Laos, karena kedua kejahatan pada kedua negara tersebut meningkat. Untuk kasus Myanmar skor kriminalitas naik dari 7,59 pada tahun 2021 menjadi 8,515 pada tahun 2023. angka tersebut menjadi skor tertinggi di dunia. Di Laos, pusat penipuan daring terkonsentrasi di Kawasan Ekonomi Segitiga Emas,, yaitu Provinsi Bokeo (Global Organized Crime Index, 2026). Korbannya tidak berhenti pada warga dalam negri melainkan warga negara ASEAN lainnya seperti Indonesia, Malaysia, Singapura, Filipina, Thailand, dan Vietnam, sebagian pekerja paksa di Laos juga berasal dari negara-negara tersebut (Sari, 2024; UNODC, 2023). Keberhasilan dari penanganan kejahatan pada Myanmar dan Laos dapat dirasakan secara langsung oleh negara-negara tetangganya.

Kapasitas Myanmar dan Laos untuk menangani kejahatan siber masih tertinggal jauh dengan Singapura dan Malaysia (Dobberstein et al., 2018), padahal seluruh negara tersebut terikat pada perangkat yang sama yaitu, SOMTC, Working Group on Cybercrime, dan ASEAN Regional CERT.

Nilai analitis terbesar terletak pada perbedaan kedua negara tersebut. Di Myanmar konflik pascakudeta 2021 dan terpecahnya kendali wilayah membuat negara sulit untuk menangani ke lokasi kejahatan siber terjadi. Laos menguasai wilayahnya, tetapi pengawasannya atas kawasan ekonomi khusus lemah. Satu rezim regional dengan dua kondisi domestik yang berbeda tersebut dapat menguji asumsi apakah efektivitas penanganan kejahatan siber dapat dilakukan dengan kerja sama dan kemauan politik atau oleh konflik dan kesenjangan kapasitas penanganan.

Berdasarkan latar belakang tersebut, penelitian ini bermaksud mengkaji secara mendalam peran ASEAN sebagai organisasi internasional dalam menangani kejahatan transnasional, khususnya di *domain cybersecurity*. Penelitian ini relevan tidak hanya dari sisi akademis dalam memperkaya literatur kajian keamanan regional Asia Tenggara, tetapi juga dari sisi praktis, yakni memberikan rekomendasi kebijakan bagi penguatan mekanisme kerja sama siber ASEAN di masa mendatang.

Atas dasar uraian latar belakang, maka dalam penelitian ini berfokus pada kajian dengan judul: *Peran ASEAN dalam Penanganan Kejahatan Siber di Kawasan Asia Tenggara: Studi Kasus Myanmar dan Laos*, melalui 4 (empat) pendekatan, yaitu: *Neoliberal Institutionalism* yang dikembangkan oleh Robert O. Keohane (1984); *Regime*

Theory yang diperkenalkan oleh Stephen Krasner (1983); *Securitization Theory* dari Mazhab Kopenhagen yang dikembangkan Barry Buzan, Ole Wæver, dan Jaap de Wilde (1998); dan *Regional Security Complex Theory* (RSCT) dari Barry Buzan dan Ole Wæver.

1.2 Pertanyaan Penelitian

Mengacu pada latar belakang tersebut di atas, maka penulis menetapkan rumusan masalah penelitian ini adalah: “Bagaimana Peran ASEAN dalam penanganan kejahatan Siber Kawasan Asia Tenggara terutama di Myanmar dan Laos.” Dari rumusan masalah tersebut, selanjutnya penulis jabarkan ke dalam beberapa pertanyaan penelitian sebagai berikut:

1. Bagaimana perkembangan kejahatan Siber di ASEAN terutama di Myanmar dan Laos?
2. Bagaimana kebijakan yang diambil oleh ASEAN dalam Menghadapi kejahatan Siber di ASEAN terutama Myanmar dan Laos?

1.3 Ruang Lingkup dan Batasan Penelitian

Pembahasan mengenai kejahatan transnasional dan *cybersecurity* di lingkup ASEAN cukup luas, serta terjadi kesenjangan kapasitas siber antarnegara anggota, seperti contoh Singapura dan Malaysia memiliki infrastruktur yang jauh lebih maju dibandingkan Laos dan Myanmar menciptakan ketidakmerataan dalam implementasi kebijakan bersama (Dobberstein et al., 2018), sehingga peneliti mencoba mengkaji inisiatif ASEAN melalui kelembagaan dalam menangani *cybersecurity*, dengan melalui pendekatan *Neoliberal Institutionalism* (Keohane, 1984), Regime Theory (Krasner, 1983) dan Securitization Theory (Buzan et al., 1998). Penelitian dilakukan dalam rentang waktu diantara tahun 2021 sampai tahun 2025.

1.4 Tujuan dan Kegunaan Penelitian

1.4.1 Tujuan Penelitian

Berdasarkan pertanyaan penelitian tersebut, maka penelitian ini mempunyai tujuan sebagai berikut:

1. Menggambarkan peran ASEAN dalam keamanan siber di Asia Tenggara.
2. Menganalisis kejahatan siber di ASEAN dengan kasus Myanmar dan Laos.
3. Menganalisis kebijakan yang diambil oleh ASEAN dalam Menghadapi kejahatan siber di Myanmar dan Laos.

1.4.2 Kegunaan Penelitian

Penelitian ini memiliki arti penting sehingga layak untuk diangkat sebagai skripsi. Dengan dilakukannya penelitian ini bertujuan untuk memberikan sebuah manfaat yaitu:

1. Manfaat Akademis, diharapkan penelitian ini dapat menjadi referensi sekaligus memberikan informasi dan pembelajaran baik untuk bidang akademik maupun untuk umum, sehingga dapat di jadikan sebagai acuan atau referensi di masa mendatang.
2. Manfaat bagi penulis, berfungsi sebagai media pengembangan kemampuan dalam bidang keilmuan yang diperoleh selama sesi kuliah dan dirangkai dalam untuk tulisan, yang juga sebagai pemenuhan dari syarat ujian program strata 1 (S1) di Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Politik, Universitas Pasundan.

1.5 Kerangka Teoritis-Konseptual

Kerangka teoritis di sini berarti mengidentifikasi teori-teori yang menjadi landasan berpikir dalam penelitian ini, sekaligus kerangka referensi untuk mengkaji permasalahan yang diangkat. Penulis perlu memaparkan teori dan konsep dari para ahli yang relevan dengan objek penelitian, agar dapat merumuskan hipotesis serta menjelaskan variabel-variabel fenomena hubungan internasional sesuai dengan judul penelitian ini.

1.5.1 Regime Theory

Dalam *International Regimes* (1983), Stephen D. Krasner mendefinisikan rezim internasional sebagai seperangkat prinsip, norma, aturan, dan prosedur pengambilan keputusan, baik implisit maupun eksplisit, yang menjadi titik temu ekspektasi para aktor dalam suatu area hubungan internasional tertentu (Krasner, 1983). Definisi ini menunjukkan bahwa rezim bukan sekadar organisasi formal dengan gedung dan sekretariat, melainkan tatanan normatif yang aktif memengaruhi perilaku negara lewat pelembagaan ekspektasi bersama.

Krasner membedakan empat komponen rezim secara hierarkis. *Prinsip* adalah keyakinan tentang fakta, kausalitas, dan kebenaran yang menjadi fondasi dari keseluruhan rezim. *Norma* adalah standar perilaku yang didefinisikan dalam kerangka hak dan kewajiban. *Aturan* adalah preskripsi atau proskripsi tindakan yang lebih spesifik. *Prosedur pengambilan keputusan* adalah praktik-praktik berlaku dalam membuat dan melaksanakan pilihan kolektif (Krasner, 1983). Hierarki ini penting: perubahan pada prinsip dan norma

berarti perubahan rezim itu sendiri, sementara perubahan pada aturan dan prosedur hanya berarti perubahan di dalam rezim.

Lebih lanjut, Krasner (1999) dalam *Sovereignty: Organized Hypocrisy* memperkenalkan konsep kritis bahwa bahkan rezim yang tampaknya kuat pun dapat menghasilkan *organized hypocrisy* kesenjangan sistematis antara komitmen normatif yang dideklarasikan secara publik dan praktik aktual yang dilakukan negara-negara anggota di lapangan. Konsep ini sangat relevan dan akan berulang kali muncul dalam analisis ASEAN.

Bila keempat komponen Krasner diproyeksikan secara langsung ke arsitektur kelembagaan ASEAN di bidang cybersecurity, peta berikut terbentuk:

Pertama, pada level prinsip: ASEAN secara kolektif mengakui bahwa kejahatan siber merupakan ancaman lintas batas yang tidak dapat ditangani secara unilateral, dan bahwa kedaulatan siber setiap negara anggota harus dihormati dalam kerangka kerja sama kolektif. Prinsip ini tercermin dalam ASEAN Political-Security Community Blueprint 2025 yang secara eksplisit menempatkan cybersecurity sebagai bagian dari agenda keamanan regional bersama (Krasner, 1983).

Kedua, pada level norma: ASEAN Way yang mencakup non-intervensi, konsensus, dan kesukarelaan tetap menjadi norma dominan yang mewarnai seluruh mekanisme kerja sama siber. Ini berarti tidak ada negara yang dapat dipaksa mengadopsi standar tertentu tanpa persetujuannya, dan tidak ada badan supranasional yang memiliki otoritas memaksa kepatuhan (Alviyani et al., 2022; IISS, 2023). Norma ini sekaligus menjadi kekuatan (menjaga kohesi organisasi) sekaligus kelemahan (membatasi efektivitas respons kolektif).

Ketiga, pada level aturan: ASEAN telah membangun instrumen konkret yang semakin spesifik dari waktu ke waktu. ASEAN Cybersecurity Cooperation Strategy (ACCS) 2017–2020 menetapkan kerangka kerja awal (ASEAN Secretariat, 2017a); ACCS 2021–2025 memperbarui dan memperluas cakupannya ke dalam lima pilar strategis: kapasitas siber, norma siber, diplomasi siber, koordinasi CERT, dan kerja sama dengan mitra eksternal (ASEAN Secretariat, 2021a). SOMTC Working Group on Cybercrime yang dibentuk tahun 2013 berfungsi sebagai forum operasional untuk harmonisasi kebijakan.

Keempat, pada level prosedur: pengambilan keputusan dilakukan melalui ASEAN Ministerial Meeting on Transnational Crime (AMMTC) yang bersidang setiap dua tahun, didukung oleh Senior Officials Meeting on Transnational Crime (SOMTC) yang bersidang lebih reguler sebagai badan teknis persiapan (Nguyen et al., 2024).

Pembentukan ASEAN Regional Computer Emergency Response Team (ASEAN CERT) pada tahun 2022 merupakan milestone paling konkret dari perkembangan rezim

cybersecurity ASEAN. ASEAN CERT berfungsi sebagai platform koordinasi teknis antarnegara anggota untuk respons insiden siber, berbagi informasi ancaman (*threat intelligence sharing*), dan peningkatan kapasitas (CSA, 2022). Ini adalah pertama kalinya ASEAN memiliki badan operasional bukan sekadar forum dialog yang secara khusus menangani cybersecurity secara kolektif.

Namun, bukti empiris juga mengonfirmasi keterbatasan rezim ini. Laporan *INTERPOL ASEAN Cyberthreat Assessment 2021* mencatat bahwa meski mekanisme formal SOMTC telah berjalan lebih dari dua dekade, berbagi informasi ancaman antarnegara masih bersifat *ad hoc* dan tidak sistematis (INTERPOL, 2021). Negara dengan kapasitas siber tinggi seperti Singapura cenderung lebih aktif berkontribusi, sedangkan negara berkapasitas terbatas seperti Laos atau Kamboja lebih banyak jadi penerima bantuan, kondisi yang persis menggambarkan apa yang Krasner (1999) sebut *organized hypocrisy*: prinsip kerja sama setara dideklarasikan di atas kertas, tetapi praktiknya timpang.

Fenomena pusat penipuan siber (*scam centers*) terorganisir di Kamboja, Laos, dan Myanmar yang beroperasi tanpa hambatan lintas batas selama bertahun-tahun meski ASEAN telah memiliki deklarasi pencegahan *cybercrime* sejak 2017 (ASEAN Secretariat, 2017b) menunjukkan secara jelas kesenjangan antara komitmen normatif dan implementasi aktual rezim ini (Huang, 2024).

Regime Theory efektif menjelaskan *mengapa* negara-negara ASEAN dengan kepentingan berbeda tetap berkomitmen pada kerangka bersama: rezim menciptakan konvergensi ekspektasi yang mereduksi ketidakpastian dan membuat perilaku satu sama lain lebih terprediksi (Krasner, 1983). Namun teori ini kurang memadai dalam menjelaskan *bagaimana* mengatasi defisit penegakan (*enforcement deficit*) yang menjadi akar masalah efektivitas ASEAN. Di sinilah *Neoliberal Institutionalism* menawarkan pelengkap yang lebih mekanistik.

1.5.2 Neoliberal Institutionalism

Dalam *After Hegemony: Cooperation and Discord in the World Political Economy* (1984), Robert O. Keohane membangun argumen bahwa kerja sama antarnegara yang berkelanjutan tetap mungkin terjadi bahkan dalam kondisi anarki internasional dan tanpa hegemon tunggal, asalkan institusi internasional yang ada mampu menjalankan fungsi-fungsi spesifik untuk mempermudah kerja sama tersebut (Keohane, 1984). Ia menolak pesimisme realis yang menganggap kerja sama selalu rapuh karena kekhawatiran *relative*

gains; sebaliknya, Keohane berpendapat negara-negara rasional bisa berfokus pada *absolute gains* selama institusi menyediakan kondisi yang tepat (Grieco, 1988; Keohane & Martin, 1995).

Keohane mengidentifikasi tiga fungsi penting institusi internasional: mengurangi biaya transaksi (*transaction costs*), sebab institusi menyediakan platform permanen sehingga negara tak perlu bernegosiasi bilateral dari nol setiap kali insiden atau isu baru muncul; menyediakan informasi yang simetris, karena institusi mengurangi kesenjangan informasi antarnegara sehingga ketidakpastian tentang niat dan perilaku pihak lain berkurang jauh; serta membangun reputasi kepatuhan lewat interaksi berulang, negara yang konsisten memenuhi komitmennya membangun reputasi sebagai aset diplomatik, sementara yang melanggar menanggung biaya reputasional (Keohane, 1984; Keohane & Martin, 1995).

Keohane & Nye (1977) dalam *Power and Interdependence* memperkenalkan konsep *complex interdependence*: pada dunia yang keterkaitannya berlapis-lapis, isu-isu non-militer seperti ekonomi, lingkungan, dan kejahatan transnasional makin penting, jalur hubungan antarnegara makin beragam dan tidak lagi terbatas pada saluran diplomatik formal, sementara kekuatan militer justru jadi instrumen yang kurang relevan untuk menyelesaikan persoalan semacam itu (Keohane & Nye, 1977).

Diterapkan pada konteks ASEAN dan *cybersecurity*, kerangka Keohane menghasilkan sejumlah proposisi analitik yang bisa diuji secara empiris.

Pengurangan biaya transaksi terjadi melalui keberadaan forum-forum permanen ASEAN. Tanpa SOMTC *Working Group on Cybercrime*, setiap kali terjadi insiden siber lintas batas misalnya serangan terhadap infrastruktur perbankan yang melibatkan dua atau lebih negara ASEAN setiap negara harus memulai negosiasi bilateral dari nol. Keberadaan forum SOMTC menciptakan prosedur standar yang memotong biaya-biaya transaksional ini secara signifikan (Keohane, 1984; ASEAN, t.t.). Pembentukan ASEAN CERT pada 2022 semakin mempertegas fungsi ini: kini ada platform teknis terpadu yang memungkinkan koordinasi respons insiden secara *real-time* tanpa harus melalui jalur diplomatik yang panjang (CSA, 2022).

Penyediaan informasi simetris tampak dalam berbagai bentuk. Laporan *INTERPOL ASEAN Cyberthreat Assessment* yang terbit berkala memberi gambaran ancaman siber kawasan yang bisa diakses seluruh negara anggota secara setara, termasuk negara dengan kapasitas intelijen siber terbatas (INTERPOL, 2021). Redistribusi informasi semacam ini

kemungkinan besar tidak akan terjadi secara sukarela di antara negara-negara dengan kemampuan yang jauh berbeda, seandainya ASEAN tidak hadir sebagai mediator.

Interaksi berulang dan reputasi kepatuhan tampak dari pola partisipasi negara-negara ASEAN dalam AMMTC dan SOMTC. Negara-negara yang konsisten hadir dan berkontribusi aktif terutama Singapura, Malaysia, dan Thailand membangun reputasi sebagai mitra teroercaya, dan reputasi itu mempermudah mereka meraih dukungan untuk inisiatif kebijakan baru (Nguyen et al., 2024). Ketidakhadiran atau sikap pasif suatu negara di forum ini, sebaliknya, bisa mengirim sinyal negatif tentang komitmen nasionalnya (Keohane, 1989).

Konsep *complex interdependence* Keohane & Nye sangat relevan untuk menggambarkan kondisi ASEAN hari ini. Pada 2022, ekonomi ASEAN mencapai lebih dari 3,6 triliun dolar AS, dengan ekosistem *e-commerce* dan *FinTech* yang tumbuh pesat di seluruh kawasan (ASEANstats, 2024). Interkoneksi sistem pembayaran digital, rantai pasok regional, dan infrastruktur data *cloud* yang melampaui batas negara menciptakan kondisi di mana serangan siber terhadap satu negara secara otomatis menghasilkan efek riak (*spillover effect*) ke negara-negara lain (Keohane & Nye, 1977).

Kasus konkret: ketika infrastruktur perbankan Bangladesh diretas melalui sistem SWIFT pada 2016 dengan kerugian 81 juta dolar AS, analisis forensik menunjukkan bahwa rute transaksi ilegal melewati beberapa yurisdiksi Asia Tenggara termasuk Filipina (Sari, 2024). Ini adalah demonstrasi nyata bahwa keamanan siber satu negara ASEAN berdampak langsung pada stabilitas sistem keuangan negara lain persis seperti yang diprediksi oleh logika *interdependence* Keohane.

Lebih lanjut, operasi INTERPOL *ASEAN Joint Operations against Cybercrime* (ASEAN AJOC) yang digelar secara berkala misalnya *Operation Synergia* dan *Operation First Light* menunjukkan bahwa kerja sama institusional telah menghasilkan hasil operasional nyata: ratusan tersangka ditangkap, jaringan *scam center* terbongkar, dan aset kejahatan disita (INTERPOL, 2021). Tanpa platform institusional ASEAN sebagai koordinator, operasi lintas yurisdiksi semacam ini secara logistik hampir mustahil dilaksanakan (Keohane, 1984).

Neoliberal Institutionalism unggul menjelaskan bagaimana institusi mempermudah kerja sama di antara negara-negara yang rasional dan saling bergantung. Asumsi rasionalitas aktor, meski begitu, punya batas penting dalam konteks ASEAN: tidak semua negara anggota bertindak sebagai aktor rasional tunggal yang sepenuhnya terbuka soal kalkulasi kepentingannya (Jervis, 1999). Negara dengan sistem pemerintahan kurang

terbuka seperti Myanmar atau Vietnam mungkin punya pertimbangan domestik yang tidak sepenuhnya bisa dijelaskan lewat kalkulasi *absolute gains* semata, soal inilah *Securitization Theory* menawarkan dimensi analitik yang lebih konstruktif, dengan fokus pada bagaimana makna dan ancaman dikonstruksikan secara sosial.

1.5.3 Securitization Theory

Securitization Theory dari Mazhab Kopenhagen (*Copenhagen School*) sebagaimana dirumuskan dalam *Security: A New Framework for Analysis* (Buzan et al., 1998) menawarkan pergeseran epistemologis yang fundamental: keamanan bukan kondisi objektif yang melekat pada suatu ancaman, melainkan hasil dari proses intersubjektif di mana aktor tertentu yang disebut *securitizing actor* berhasil meyakinkan audiens bahwa suatu isu merupakan ancaman eksistensial yang memerlukan tindakan darurat di luar prosedur politik normal.

Konsep inti adalah *securitizing move* atau *speech act* (tindak tutur keamanan): pernyataan diskursif yang mengangkat suatu isu dari ranah *politics* (politisasi biasa) ke ranah *security* (sekuritisasi), dengan mengklaim bahwa isu tersebut mengancam eksistensi suatu *referent object* bisa berupa negara, masyarakat, individu, sistem ekonomi, atau ekosistem (Buzan et al., 1998). Sekuritisasi dinyatakan berhasil bukan hanya ketika *speech act* diucapkan, tetapi ketika audiens menerima konstruksi tersebut dan mendukung langkah-langkah luar biasa (*extraordinary measures*) untuk menanganinya.

Penting untuk membedakan tiga level: *non-politicized* (isu tidak menjadi perhatian publik atau negara), *politicized* (isu ditangani melalui prosedur kebijakan normal), dan *securitized* (isu dikonstruksikan sebagai ancaman eksistensial yang memerlukan respons darurat melampaui prosedur normal) (Buzan et al., 1998). Buzan et al. juga memperkenalkan *facilitating conditions* kondisi-kondisi kontekstual yang mempermudah atau menghambat keberhasilan sekuritisasi serta gagasan tentang *desecuritization* sebagai proses mengembalikan isu dari ranah keamanan ke ranah kebijakan normal.

Dalam konteks ASEAN, proses sekuritisasi *cybercrime* dapat ditelusuri secara historis sebagai proses bertahap yang berlangsung selama lebih dari dua dekade, dengan identifikasi komponen-komponen berikut:

Aktor sekuritisasi dalam kasus ini adalah para pemimpin negara anggota ASEAN secara kolektif, ASEAN Secretariat sebagai institusi, serta negara-negara dengan kapasitas siber tinggi seperti Singapura yang kerap menjadi promotor agenda keamanan siber di forum regional (IISS, 2023). Dalam konteks eksternal, tekanan normatif dari *UN Group of*

Governmental Experts on Developments in the Field of ICTs (UNGGE) serta INTERPOL turut menjadi aktor pendorong (INTERPOL, 2021).

Objek referensi dalam sekuritisasi *cybercrime* ASEAN bersifat multidimensi: pada level negara, objek referensinya adalah infrastruktur kritis nasional (sistem perbankan, jaringan energi, sistem pemerintahan digital); pada level regional, objek referensinya adalah stabilitas ekonomi kawasan dan kepercayaan terhadap ekosistem digital ASEAN; pada level masyarakat, objek referensinya adalah keselamatan individu dari penipuan siber dan eksploitasi digital (Buzan et al., 1998; Sari, 2024).

Audiens adalah sepuluh negara anggota ASEAN beserta mitra dialog (Tiongkok, Amerika Serikat, Jepang, Australia, dll.) yang harus menerima konstruksi ancaman tersebut dan mendukung langkah-langkah kolektif melampaui kerja sama teknis biasa (Alviyani et al., 2022).

Proses sekuritisasi *cybercrime* di ASEAN dapat dibagi menjadi tiga fase yang dapat diidentifikasi secara empiris:

Fase Politisasi (1999–2012): *Cybercrime* mulai dimasukkan sebagai salah satu dari sepuluh area kerja SOMTC sejak 2001, namun masih diperlakukan sebagai isu teknis-administratif dalam kategori *low politics* (Sundram, 2024). Pada fase ini belum ada *speech act* yang mengangkat isu ini ke level ancaman eksistensial.

Fase Sekuritisasi Parsial (2013–2017): Pembentukan SOMTC *Working Group on Cybercrime* pada 2013 dan pengadopsian *ASEAN Declaration to Prevent and Combat Cybercrime* pada 2017 merepresentasikan *securitizing moves* yang semakin eksplisit (ASEAN Secretariat, 2017b). Deklarasi 2017 ini dapat dibaca sebagai *speech act* formal kolektif pertama yang secara eksplisit mengkonstruksikan *cybercrime* bukan sekadar pelanggaran hukum biasa, melainkan ancaman terhadap stabilitas kawasan yang memerlukan respons kolektif terkoordinasi.

Fase Sekuritisasi Penuh (2018–sekarang): *ASEAN Leaders' Statement on Cybersecurity Cooperation* (2018) adalah momen paling signifikan di mana sekuritisasi mencapai level kepala pemerintahan secara kolektif. Pernyataan ini mengangkat *cybersecurity* secara eksplisit sebagai isu keamanan regional bukan hanya isu teknis dan menyerukan koordinasi yang lebih intensif (ASEAN Secretariat, 2021a). Pembentukan

ASEAN CERT pada 2022 adalah wujud *extraordinary measure* pertama yang konkret, melampaui mekanisme dialog biasa menuju badan operasional bersama (CSA, 2022).

Kondisi fasilitasi yang memperkuat sekuritisasi ini mencakup lonjakan insiden siber pasca-2020 yang dipicu oleh percepatan digitalisasi selama pandemi COVID-19; kerugian ekonomi dari penipuan siber lintas batas yang mencapai miliaran dolar laporan INTERPOL mencatat korban dari seluruh kawasan (INTERPOL, 2021) serta menguatnya tekanan norma global dari kerangka UN dan UNGGE yang mendorong negara-negara memperlakukan *cybersecurity* sebagai isu keamanan nasional serius.

Analisis *securitization* juga mengungkap paradoks mendasar dalam konteks ASEAN. Di satu sisi, sekuritisasi berhasil dilakukan pada level *speech act* dan komitmen politik: para pemimpin ASEAN secara konsisten menyatakan bahwa *cybercrime* adalah ancaman eksistensial. Di sisi lain, *extraordinary measures* yang seharusnya menjadi konsekuensi logis sekuritisasi yang berhasil seperti kewajiban hukum mengikat, mekanisme sanksi terhadap negara yang tidak patuh, atau pembentukan badan supranasional dengan otoritas memaksa justru tidak terwujud karena terhambat oleh norma non-intervensi *ASEAN Way* (Buzan et al., 1998; Krasner, 1999).

Inilah yang dapat disebut sebagai *securitization* tanpa *extraordinary measures*: kondisi di mana isu telah berhasil dikonstruksikan sebagai ancaman eksistensial, tetapi respons kebijakan yang dihasilkan masih berkuat pada ranah prosedur normal (pembentukan *working group*, deklarasi sukarela, program *capacity building*). Fenomena ini merupakan kontribusi analitik orisinal penelitian ini terhadap literatur kajian keamanan regional ASEAN.

Divergensi definisi juga menjadi hambatan desekuritisasi yang signifikan: negara-negara ASEAN belum memiliki konsensus tentang apa yang dimaksud dengan "serangan siber" yang memerlukan respons kolektif, berbeda dengan definisi "serangan bersenjata" dalam hukum internasional konvensional yang memiliki tradisi yurisprudensi lebih panjang (Sari, 2024). Tanpa definisi bersama, koordinasi respons kolektif selalu berpotensi terhambat oleh perbedaan interpretasi.

1.5.4 Regional Security Complex Theory

Regional Security Complex Theory (RSCT) adalah konsep hubungan internasional oleh Barry Buzan dan Ole Wæver. Teori ini menjelaskan bahwa masalah keamanan suatu negara sangat terikat dengan negara tetangga, menciptakan klaster geografis di mana ancaman tidak bisa ditangani secara mandiri. Konsep kompleks keamanan kawasan membahas terpusatnya keamanan di wilayah-wilayah yang terbentuk secara geografis.

Persoalan keamanan sulit menyebar secara luas, dan ancaman sangat mungkin muncul di dalam kawasan tersebut. Keamanan setiap pelaku di sebuah kawasan berinteraksi dengan keamanan pelaku lain. Biasanya terdapat interdependensi keamanan yang tinggi di dalam suatu kawasan; interdependensi lintas kawasan justru tidak terjadi. Itulah hal yang mendefinisikan sebuah kawasan dan menjadikan keamanan kawasan sebuah bidang studi yang unik. Adakalanya negara pinggiran memisahkan dua kawasan, contohnya Afghanistan yang terletak di antara Timur Tengah dan Asia Selatan. Kawasan harus diperlakukan sebagai sistem kecil yang membuat semua teori hubungan internasional mampu diterapkan, misalnya keseimbangan kekuasaan, polaritas, interdependensi, sistem aliansi, dll.

Ide Kompleks Keamanan Regional diciptakan oleh Barry Buzan dan Ole Waever, yang berasumsi masalah keamanan dapat dikelompokkan ke dalam kompleks regional yang terpisah secara geografis. Mereka menganggap bahwa masalah keamanan jarang menjadi sangat penting ketika jaraknya jauh; bahaya serupa sebagian besar ditemui di wilayah yang sama. Saling ketergantungan antar aktor di wilayah yang sama jauh lebih kuat daripada antar aktor dari wilayah yang berbeda atau antar daerah secara keseluruhan. Teori ini juga menekankan peran kekuatan global dan regional di dunia pasca-Perang Dingin.

Regional Security Complex muncul sebagai suatu konsep baru untuk struktur keamanan internasional sebagai dimensi yang menghubungkan pola kehidupan antar negara di kehidupan internasional pada saat sebelum perang dingin, saat terjadi perang dingin dan pasca perang dingin. Regional Security Complex memberikan pandangan yang berbeda serta beragam namun memiliki pengaruh yang cukup teoritis (Barry Buzan and Ole Weaver, 2003: 43-44).

Dalam suatu Regional Security Complex permasalahan mengenai keamanan negara-negara yang bersangkutan berhubungan erat sehingga permasalahan mengenai keamanan nasional tidak mungkin ada tanpa memperhitungkan mengenai keamanan wilayah, walaupun terdapat ketergantungan antar negara di suatu kawasan bukan berarti keadaan yang harmonis akan tercapai bahkan hubungan antar negara dalam suatu kawasan selalu dipengaruhi oleh berbagai macam hal seperti: perimbangan kekuatan, aliansi dengan negara lain serta masuknya suatu kekuatan eksternal di dalam kawasan tersebut (Barry Buzan and Ole Weaver, 2003: 47).

Barry Buzan dan Ole Waever merumuskan dua variabel penyusun essential dari teori Regional Security Complex yakni: (Barry Buzan and Ole Weaver, 2003: 53). *Pertama*, Variabel internal yang dapat diukur menggunakan beberapa indikator, yaitu: a)

Letak geografis. Dalam letak geografis yang menjadi fokus adalah dengan melihat seberapa besar peranan letak geografis dalam mendefinisikan suatu negara sebagai suatu kawasan. Karena tidak semua negara yang letaknya berdekatan itu dapat menjalin suatu pengaturan keamanan bersama. b) Interaksi antar negara. Sedangkan interaksi antar negara ini akan melihat seberapa sering dan seberapa dekat hubungan (interaksi) antar negara-negara dalam suatu kawasan. Fokusnya kemudian dengan melihat juga apakah interaksi antar negara begitu dalam sehingga mereka merasa sebagai satu kesatuan. Ataukah justru interaksi yang terlalu sedikit itu dapat membuat mereka berpersepsi bahwa mereka tidak mengenal negara tetangganya sendiri. c) Kesamaan system. Dalam kesamaan sistem ini, yang dilihat adalah dari berbagai kesamaan sistem budaya, ekonomi, sosial dan politik dalam negara-negara di satu kawasan. Semakin banyak negara-negara tersebut memiliki kesamaan yang semakin kompleks juga, tentunya ini akan dapat menumbuhkan rasa solidaritas yang semakin kuat pula.

Kedua, Variabel eksternal dapat diukur menggunakan dua indikator, yaitu: a) Situasi internasional. Indikator ini melihat bagaimana kondisi atau keadaan lingkungan internasional. Apakah keadaan lingkungan internasional saat itu mendukung atau tidaknya untuk terbentuknya pengaturan keamanan (security arrangement) dalam Regional Security Complex (RSC). Seperti ketika kondisi dunia dikuasai oleh kekuatan Amerika Serikat, hal ini kemudian mendorong Rusia, China dan negara-negara di kawasan Asia Tengah untuk membentuk suatu pengaturan politik dan keamanan bersama untuk melawan dominasi Amerika Serikat tersebut. b) Isu-isu yang sedang berkembang. Indikator yang terakhir ini terkait dengan isu-isu yang berkembang. Apakah saat ini di dunia sedang berkembang isu-isu yang membutuhkan Kerjasama negara kawasan terutama dalam hal pengaturan keamanan atau tidak. Seperti ketika isu terorisme yang sedang mencuat, yang pada akhirnya menuntut negara-negara dalam satu kawasan untuk membuat security arrangement. Atau justru isu yang sedang berkembang ternyata tidak berpengaruh pada pembentukan pengaturan keamanan antar negara Kawasan. (Nofita Andes Nurdiana, 2018)

Regional Security Complex Theory adalah teori yang memadukan pendekatan neorealis dan konstruktivis untuk melihat kompleksitas keamanan kawasan. Pendekatan neorealis digunakan untuk melihat peran power distribution dan faktor geografis dalam kawasan yang dimaksud. Sementara pendekatan konstruktivis digunakan untuk mengidentifikasi pola amity dan enmity yang membentuk kompleksitas keamanan di kawasan. Secara utuh Regional Security Complex memiliki variabel-variabel sebagai berikut: boundary dalam Regional Security Complex, social construction dan pola amity

dan enmity negara-negara di dalam kawasan, anarchic stucture atau struktur anarki dalam sistem kawasan, serta polaritas atau power distribution di dalam kawasan (Buzan, 2003: 53).

1.6 Kerangka Analisis

Mengacu pada Kerangka Teoritis-Konseptual dan asumsi penelitian, maka penulis memandang bahwa penanganan kejahatan transnasional dan *Cybersecurity* di ASEAN perlu terlembagakan dalam sebuah rezim di kawasan sebagai upaya meningkatkan efektivitas penanganan. Faktanya, negara-negara ASEAN masih berbeda pola tindak dan kapasitas sibernya, kesenjangan yang menciptakan ketidakmerataan dalam implementasi kebijakan bersama (Dobberstein et al., 2018; IISS, 2023). Ketiadaan instrumen hukum yang mengikat di tingkat regional pun membuat kerja sama siber ASEAN lebih bergantung pada itikad baik negara anggota ketimbang kewajiban hukum formal (Huang, 2024).

Permasalahan Kejahatan Transnasional dan *Cybersecurity* di negara-negara ASEAN terutama berkaitan dengan peredaran narkoba dan obat-obat terlarang yang semakin meningkat dalam hal jenis dan modus operandi penyelundupan narkotika di kawasan Asia Tenggara; di samping itu jaringan narkotika di Asia Tenggara memiliki mata rantai yang rapi dan terorganisir (Sundram, 2024). ASEAN telah melakukan berbagai macam kesepakatan penanganan terkait peredaran narkotika, seperti *Annual Ministerial Meeting on Transnational Crime* (AMMTC), *ASEAN Chiefs of National Police* (ASEANAPOL) dan kerja sama pemutusan mata rantai penyelundupan narkotika di wilayah perairan *ASEAN Seaport Interdiction Task Force* (SITF), sampai pada pusat kerja sama dan pertukaran informasi terkait penyelundupan narkotika di wilayah Asia Tenggara yaitu *ASEAN Narcotics Cooperation Centre* (ASEAN-Narco) (ASEAN Secretariat, 2016).

Kebijakan-kebijakan ASEAN ini, sayangnya, belum optimal, sebab hanya berfokus pada upaya antisipasi yang parsial dan domestik oleh masing-masing negara. Akibatnya, negara yang paling ketat dan kuat menjalankan operasi penanganan penyelundupan narkotikalah yang paling efektif menangani kejahatan transnasional ini di Asia Tenggara, bukan ASEAN sebagai satu kesatuan. Nilai dan norma terhadap ancaman bersama narkotika belum terlembaga, sehingga penanganan tetap berpusat pada negara mana yang paling merasakan dampak negatifnya. Alhasil, upaya penanganan bersama terhadap kejahatan transnasional penyelundupan narkotika masih bersifat parsial dan belum menyentuh optimal peran ASEAN sebagai komunitas bersama (*regime*) dalam menangani persoalan ini di kawasan Asia Tenggara (Sundram, 2024).

Berkaitan dengan pentingnya rezim dalam menangani kejahatan transnasional, diungkapkan oleh Stephen D. Krasner dalam *International Regimes* (1983). Krasner menjelaskan bahwa rezim internasional adalah seperangkat prinsip, norma, aturan, dan prosedur pengambilan keputusan implisit maupun eksplisit yang di sekitarnya ekspektasi para aktor berkonvergensi dalam suatu area hubungan internasional tertentu (Krasner, 1983). Definisi ini menegaskan bahwa rezim bukan sekadar organisasi formal, melainkan suatu tatanan normatif yang memengaruhi perilaku negara-negara melalui pelembagaan ekspektasi bersama.

Dalam konteks ASEAN diperlakukan sebagai rezim internasional di bidang *cybersecurity* yang memiliki empat komponen utama, yaitu: prinsip, berupa pengakuan bersama atas kedaulatan siber negara anggota dan pentingnya kerja sama kolektif; norma, berupa komitmen terhadap non-intervensi, konsensus, dan kerja sama sukarela sebagaimana tercermin dalam *ASEAN Way*; aturan: instrumen konkret seperti contohnya *ASEAN Cybersecurity Cooperation Strategy* (ACCS) 2021–2025 (ASEAN Secretariat, 2021a), *SOMTC Working Group on Cybercrime*, dan ASEAN CERT; dan prosedur, berupa mekanisme pengambilan keputusan melalui *ASEAN Ministerial Meeting on Transnational Crime* (AMMTC) dan SOMTC.

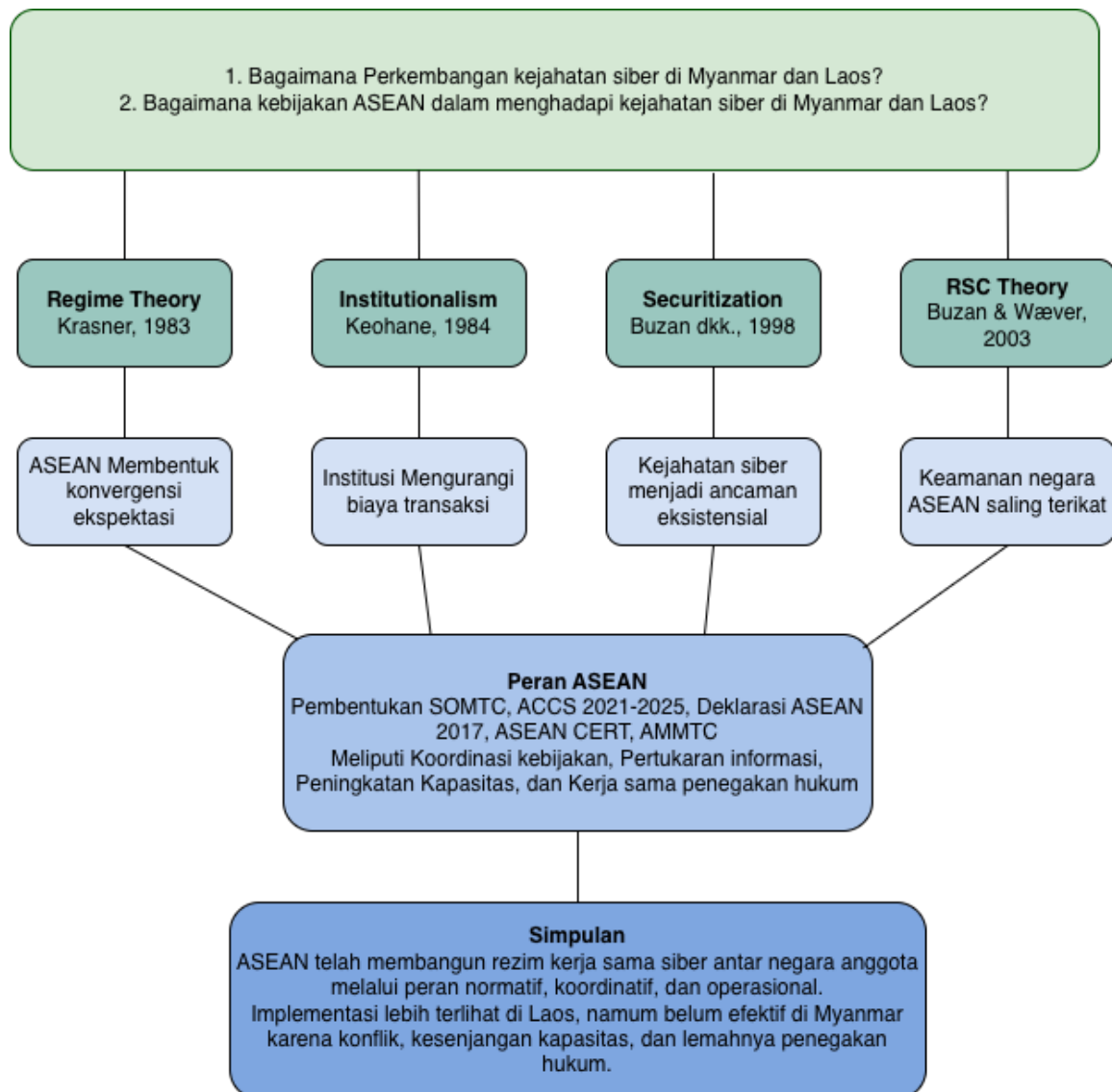
Hal ini dikuatkan oleh Robert O. Keohane dalam bukunya *After Hegemony: Cooperation and Discord in the World Political Economy* (1984), di mana Keohane memandang bahwa institusi internasional memainkan peran krusial dalam memfasilitasi kerja sama antarnegara yang rasional dan mementingkan diri sendiri, khususnya dalam kondisi saling ketergantungan (*interdependence*) yang tinggi (Keohane, 1984).

Secara komprehensif dikuatkan oleh pandangan Barry Buzan, Ole Wæver, dan Jaap de Wilde dalam *Security: A New Framework for Analysis* (1998). Konsep sentral pemikiran Buzan dan kawan-kawan adalah *securitizing move* atau *speech act* (tindak tutur keamanan): tindakan diskursif di mana seorang aktor sekuritisasi (*securitizing actor*) mengangkat suatu isu dari ranah politik biasa (*politicization*) ke ranah keamanan (*securitization*) dengan mengklaim bahwa isu tersebut merupakan ancaman eksistensial terhadap suatu objek referensi (*referent object*). Sekuritisasi dinyatakan berhasil apabila audiens menerima konstruksi tersebut dan mendukung langkah-langkah luar biasa untuk menanganinya (Buzan et al., 1998).

Oleh karenanya dalam menangani permasalahan ini, petinggi ASEAN perlu kiranya mempercepat terwujudnya lembaga khusus yang menangani kejahatan transnasional dan *Cybersecurity*, mengingat perkembangan pelaku kejahatan transnasional dan

Cybersecurity di ASEAN mengalami perkembangan yang cepat terutama berkenaan dengan jenis, modus operandi, mata rantai yang rapi serta terorganisir dengan baik (UNODC, 2023; Huang, 2024).

Gambar 1.3 Visualisasi Kerangka Analisis



1.7 Asumsi Penelitian

Penelitian ini menggunakan pendekatan kualitatif, sehingga asumsi penelitian berfungsi sebagai jawaban sementara dari pertanyaan penulis. Asumsi penelitian dirumuskan berdasarkan latar belakang, pertanyaan penelitian, dan kerangka teoritis-konseptual.

Asumsi utama dalam penelitian ini dapat dirumuskan sebagai berikut: **semakin kuat kerjasama regional ASEAN dan semakin besar kemauan negara anggota untuk menerapkan kebijakan bersama, semakin efektif penanganan kejahatan siber. Sebaliknya, semakin besar kesenjangan kapasitas antar negara anggota, lemahnya penegakan hukum, dan konflik domestik akan membatasi efektivitas peran ASEAN terhadap penanganan kejahatan siber.**