BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi digital saat ini sedang mengalami perkembangan yang sangat pesat, di mana hal ini telah membuat lanskap keamanan global juga ikut berkembang. Begitu juga pada Kawasan Asia Tenggara, di tengah kemajuan saat ini, keamanan *cyber* menjadi suatu isu yang jadi amat krusial dan tentunya tidak boleh diabaikan dengan sembarangan. Ini karena keamanan *cyber* telah menjadi isu lintas sektor di Asia Tenggara. Di mana pada awalnya hal ini hanya terfokus pada ekonomi digital, namun kini keamanan *cyber* sudah mencaup tiga pilar komunitas ASEAN yaitu politik keamanan, ekonomi, dan juga sosial-budaya. (Kristiani, n.d.) Oleh karena hal ini, segala serangan yang akan atau bahkan telah terjadi seperti serangan terhadap infrastrutur digital, kebocoran data pribadi, penyebaran disinformasi, dan peretasan sistem layanan publik haruslah segera diantisipasi. Dalam hal ini sendiri, suatu negara bahkan wilayah khususnya ASEAN harus membangun *cyber resilience* (ketahanan siber), yang mana suatu negara harus memiliki kemampuan dalam mengantisipasi, menahan, merespon, bahkan memuliki kemampuan untuk pulih secara cepat dari serangan *cyber* sambil tetap mempertahanan setiap fungsi fundamenalnya.

ASEAN sebagai organisasi regional juga sudah menyadari tentang pentingnya kerja sama dalam menghadapi ancaman *cybet*. Hal ini bisa dilihat dari inisiasi yang dilakukan oleh ASEAN, seperti *ASEAN Ministeral Conference on Cybersecurity* (AMCC) dan *ASEAN Cybersecurity Cooperation Strategy* (Novitasari 2017) . Inisiasi ini sendiri sudah mulai dilakukan sejak tahun 2016, yang mana inisiasi ini kemudian diperbarui menjadi *ASEAN Cybersecurity Cooperation Strategy 2021-2025*. Inisiasi ini bertujuan untuk membangun keamanan cyber rehional dengan meningkatkan kapasitas teknis dan memperkuat mekanisme koordinasi di antara negara anggota.

Bahkan inisiatif ini sendiri sudah sampai pada tahap kerja sama luar Kawasan dengan negara-negara lain, yaitu Jepang, Amerika Serikat, dan juga Uni Eropa. Namun, efektivitas dari banyaknya kerangka kerja ini masih perlu dipertanyakan. Ini karena masih banyak Implementasi yang terjadi di lapangan tidak sesuai karena terhambat oleh karakteristik internal kawasan itu sendiri. Seperti adanya *non-interference* dan *consensus*, juga dengan besarnya kesenjangan dalam tingkat *cyber* di antara negara anggota (Ramadhan, 2022)

Namun, efektivitas dari beberapa kerangka kerja yang dibangun oleh ASEAN masih menghadapi banyak tantangan. Salah satunya adalah ketimpangan kapasitas keamanan *cyber* yang di antara negara anggota negara ASEAN sendiri. Misalnya seperti Singapura, negara ini telah menempati posisi terdepan di antara dengan kesiapan teknis dan kebijakan yang cukup baik, dan melalui pembentukan *ASEAN-Singapore Cybersecurity Centre of Excellence*(Noor et al., n.d.). Negara ini membuat dirinya menjadi salah satu pelopor dalam keamanan *cyber* regional. Sedangkan di sisi lain, negara seperti Filipina malah menghadapi tantangan besar arena keterbatasan infrastruktur, sumber daya manusia, serta minimnya kebijakan nasional.

Filipina sendiri menjadi salah satu negara anggota ASEAN yang memiliki tantangan serius dalam bidang cyber security. Ini karena banyak rangkaian serangan insiden cyber seperti adanya peretasan sistem pemilu, kebocoran data pemerintah, penyebaran konten pornografi, penipuan digital, hingga pada serangan ransomwar. Hal inilah menunjukkan tingkat kerentangan yang cukup tinggi. Pemerintah Filipina memang telah memberikan respon berupa kebijakan seperti *National Cybersecurity Plan (NCSP) 2022* dan dilakukan pembaruan *National Cybersecurity Plan 2023-2028*, serta pemerintah Filipina juga membentuk Lembaga seperti *Departement of Information and Communiations Technology (DICT)* dan *Computer Emergency Response Team – Philippines (CERT-PH)* (Villanueva, 2023). Namun, berbagai tantangan seperti keterbatasan sumber daya manusia, koordinasi antar lintas sektor, dan

ketimpangan infrastruktur digital masih menjadi hambatan utama dalam memperkuat *cyber resilience* nasional terhadap negara ini.

Kondisi inilah yang menempatkan filipina Sebagai salah satu negara anggota ASEAN yang menjadi high-demand recipient, atau negara yang paling membutuhkan adanya intervensi, pelatihan, dan Pembangunan kapasitas teknis melalui skema ASEAN dibandingkan dengan anggota lain seperti Singapura atau Malaysia. Pada hal ini, Filipina bukan hanya rentan tapi juga menunjukkan ketidakberhasilan dalam Implementasi kebijakan nasioanl seperti NCSP 2022 yang kemudian harus diubah menjadi NCSP 2023-2028. Ini karena lemahnya koorinasi lintas Lembaga, keterbatasan SDM, dan adanya ketidakadaan mekanisme respons pada tiap insiden yang terjadi. Kegagalan ini memperlihatkan bahwa upaya domestic Filipina belum cukup untuk menciptakan ketahanan cyber tanpa dukungan eksternal.

Namun, dalam konteks kerja sama regional, Filipina turut terlibat dalam berbagai inisiatif ASEAN terkait *cyber security*. Ini termasuk forum AMCC, dialog *ASEAN Digital Minister's Meeting* (ADGMIN), dan banyaknya partisipasi dalam upaya pembentukan *ASEAN Cyber Security Center*. Meski begitu, Implementasi kerja smaa tersebut masih berupa dokumen dan pertemuan semata. Ini karena banyak tantangan yang dihadapi oleh ASEAN, seperti belum adanya harmonisasi kebijaan antarnegara, banyaknya keterbatasan kapasitas teknis nasional, serta belym terbentuknya *ASEAN Cyber-CERT* sebagai lembaga permanen regional (Brock, 2024).

Padahal, penting bagi negara-negara ASEAN untuk meresmikan hal ini. Ini karena pembentukan lembaga permanen tidak hanya akan memperkuat koordinasi lintas negara dan mempercepat respons terhadap adanya insiden *cyber,* tapi juga untuk menjadi pondasi utama bagi regional dalam mengupayakan pembangunan ketahanan *cyber* yang kolektif. Karena dalam konsep regional *cyber resilience*, kerja sama regional tentu akan sangat oenting

Ketika akan menghadapi ancaman *cyber* yang bersifat transnasional, ini dikarenakan tidak ada satu negara pun yang benar-benar bisa menangani serangan *cyber* secara uniteral. Oleh karena itu, pembentukan *ASEAN-CERT* akan sangat memainka peran kunci dalam meningkatkan *cyber resilience* kawasan ASEAN khususnya pada Filipina di tengah maraknya ancaman *cyber* yang semakin kompleks.

Selain itu juga, di antara tantangan utama dalam menerapkan langkah-langkah *cyber security* yang efektif adalah kompleksitas serangan *cyber*, ketidakadaan kerangka hukum yang komprehensif, serta masih banyak kebutuhan mendesa akan peningkatan kesadaran dan keahlian dalam bidang *cyber security*. Meski pemerintah Filipina dan ASEAN sudah memiliki strategi dalam memperkuat keamanan nasional melalui inisiatif kerjasama *cyber* yang tentu mencerminkan sifat yang proaktif. Namun, upaya-upaya ini masih kurang dalam melihat bahwa diantara kerentanan *cyber security* perlu ada infrastruktur keamanan *cyber* yang kokoh.

Ketimpangan ini tidak hanya berdampak pada kesiapan teknis dari suatu negara, tapi juga mempengaruhi komitmen politik karna menghadirkan presepsi ancaman yang nyata dan juga membuat dampak pada kawasan regional. Oleh karena itu, kondisi ini tentu berdampak langsungg pada efektivitas implementasi keranga kerja regional. Tentunya di sini, tidak semua negara memiliki kapasitas atau kepentingan yang sama dalam menerapkan kebijakan keamanan *cyber* yang akan disepakati bersama. Ketimpangan iniah yang berpotensi besar dalam menghambat adanya pelaksanaan inisiatif regional yang tentu saja membutuhkan kesiapan teknis dan politik yang juga setara. Hal ini sendiri juga dijelaskan dalam analisis (ATKearney dalam (Kristiani, n.d.)), yang mana memperlihatkan, jika ternyata banyak anggota negara di kawasan Asia Tenggara yang tergabung dalam ASEAN, menjadi sasaran utama yang paling empuk dalam kasus serangan *cyber*.

Meskipun ASEAN sudah merancang pendekatan yang inklusif dan multidimensional dalam keamanan *cyber*, namun tetap saja ketimpangan kapasitas antaregaranya masih ada. Baik itu dari sisi infrastruktur digital, sumber daya manusia, bahan sampai pada kesiapan kebijakan yang masih menjadi hambatan utama bagi efektivitas Implementasi kerjasama ini. Hal inilah yang akhirnya membuat upaya integritas dan harmonisasi kamanan *cyber* dalam lingkup ASEAN cenderung berjalan lambat dan tidak merata. Sehingga, penulis berangkat dari permasalahan tersebut dan focus terhadap bagaimana negara-negara ASEAN merespon dan menyesuaikan diri (atau tidak) terhadap regulasi *cyber* regional. Penulis akan menelaah bagaimana faktor-faktor internal lah yang menjadi peghambat-seperti keterbatasan sumber daya, perbedaan sistem politik, sampai pada perbedaan prioritas kebijakan-penelitian ini juga akan bertujuan untuk mengisi celah pemahaman terkait adanya dinamika internal di balik lambatnya internalisasi *cyber* di kawasan ASEAN. Oleh karena itu, meski inisiatif seperti *ASEAN Cybersecurity Cooperation Strategy* memang penting, namun jika tanpa perhatian khusus pada negara-negara anggota yang tertinggal secara digital, maka ASEAN justru malah berisiko menciptaan kesenjangan baru dalam tata kelola ruang *cyber* regional.

1.2 Rumusan Masalah

Melihat latar belakang tersebut, penulis sendiri akan mengangkat soal "Mengapa Filipina bekerjasama dengan ASEAN dalam upaya ketahanan siber pada tahun 2018-2024"

1.3 Tujuan Penelitian

a. Menganalisis tingkat kesiapan kelembaaan dan kapasitas teknis Filipina dalam membangun *cyber resilience* pada tahun 2018-2024.
b. Mengkaji sejauh mana kerja sama ASEAN berperan dalam mendukung ketahanan *cyber* Filipina pada periode 2018-2024.
c. Mengkaji dinamikan internal dan tantangan yang dihadapi Filipina dalam mengimplementasikan kerja sama keamanan *cyber* ASEAN.

1.4 Manfaat Penelitian

Dalam menulis penelitian ini, penulis mengharapkan adanya manfaat dalam dua kategori ini, yaitu;

1.1.1 Manfaat Teoritis

Memberikan kontribusi pada pengembangan studi keamanan non-tradisional, khususnya *cyber* dan *cyber resilience* dalam kerangka kerja sama kawasan, serta memperluas penggunaan teori securitization Barry Buzzan dalam konteks Filipina dan regional Asia Tenggara.

1.1.2 Manfaat Praktis

Memberikan gambaran bagi pemerintah Filipina dan ASEAN tentang tantangan terkait Implementasi kerja sama *cyber security*, serta menjadi masukan dalam pengambilan kebijaan yang lebih responsive dan realistis untuk memperkuat kapasitas keamanan digital nasional dan regional.

1.5 Sistematika penulisan

Dalam menyusun skripsi ini, penulis membagi dalam lima bab, dengan rincian sebagai berikut:

BAB I: Pendahuluan: Pada bagian ini, penulis memaparkan latar belakang penelitian, pertanyaan riset, tujuan penelitian, manfaat penelitian baik itu dari segi teoritik maupun dari segi praktik, kemudian ditutup dengan sistematika penulisan. Bab ini sendiri merupakan fondasi utama bagi penulis dalam mengembangkan penelitian skripsi sampai pada kesimpulan nanti.

BAB II: Tinjauan Pustaka: Pada bagian ini sendiri, penulis akan menjelaskan terkait dengan landasan teori yang penulis gunakan untuk menjawab dan menjelaskan terkait pertanyaan riset yang dimunculkan. Pada bagian ini pula, penulis juga akan menjelaskan terkait beberapa penelitian terdahulu dan gap yang ada di dalamnya.

BAB III: Metodologi Penelitian: Pada bagian ini, penulis akan menjelaskan bagaimana metode penelitian yang akan penulis gunaan untuk bsia menjawab permasalahan yang muncul.

BAB IV: Analisis dan Pembahasan: Pada bagian, penulis akan membahas terkait hasil analisis dari esiapan Filipina dalam aspek kelembagaan dan teknis, serta bagaimana evaluasi peran kerja sama ASEAN, dan integrasi dengan kerangka teori yang digunakan

BAB V: Penutup: Pada bab ini, penulis akan menyimpulan bagaimana hasil akhir yang penulis telah lakukan, serta penulis juga akan memberian jawaban atas pertanyaan riset yang telah dimunculkan. Penulis juga aanmemberikan saran bagi penelitian selajutnya.