BAB I

PENDAHULUAN

1.1 Latar Belakang

Salah satu bentuk kemajuan peradaban dunia adalah kemajuan ilmu pengetahuan dan teknologi. Kemajuan ini diharapkan akan membuat hidup manusia lebih mudah dan efisien. Luasnya arus informasi dan kemudahan akses komunikasi dengan segala sesuatu yang terhubung dengan jaringan internet menunjukkan kemajuan teknologi dan ilmu pengetahuan. Jaringan yang terhubung akan memunculkan realitas baru yang dikenal sebagai ruang siber. Karena semua individu lintas negara dan benua terhubung dan berinteraksi satu sama lain, ruang siber terbentuk karena semakin pendeknya waktu, ruang, dan jarak (Jati, 2016).

Pada masa Perang Dingin, studi keamanan hanya berfokus pada sektor keamanan bidang politik dan militer. Akan tetapi berdasarkan perkembangan zaman, sektor keamanan semakin meluas dengan masuknya isu lingkungan, ekonomi dan sosial (Buzan, 1998). Salah satu kemajuan teknologi yang memberikan pengaruh besar adalah internet yang merupakan sebuah jaringan komunikasi. Perkembangan teknologi yang semakin modern selalu memiliki dampak positif dan negatif. Dengan semakin terdigitalisasi, studi keamanan pun juga terpengaruh. Sebelumnya sektor keamanan hanya ada lima bidang saja akan tetapi saat ini berkembang menjadi enam bidang (Joseph S.Nye, 2011). Nye menambahkan dalam bukunya yang berjudul *The Future of Power*, *cyber* perlu mendapatkan prioritas dalam *security studies*. Ia menjelaskan bahwa dimensi kehidupan negara-bangsa di dalamnya tidak akan terlepas dari peranan internet.

Sehingga mau tidak mau, negara-bangsa perlu menambahkannya sebagai prioritas keamanan negara.

Akses terhadap komunikasi dan informasi mempunyai dampak yang sangat besar terhadap paradigma hubungan internasional. Dalam hal keamanan, internet memperluas dan memperumit tantangan terhadap kedaulatan suatu negara. Dunia tidak lagi memandang militer sebagai satu-satunya ancaman bagi suatu negara, namun justru merespons permasalahan non-militer, salah satunya adalah serangan siber.

Kemajuan teknologi dan informasi saat ini menawarkan banyak manfaat potensial, memungkinkan hampir semua orang beralih ke dunia digital dan terhubung ke internet. Teknologi internet saat ini cepat dan efisien. Namun, sebagian masyarakat belum menyadari bahwa internet mempunyai dampak negatif, salah satunya adalah kejahatan siber. Ketika semua gadget terhubung dengan internet, *Internet of Things* berkembang secara spontan. *Internet of Things* adalah sebuah konsep di mana suatu peralatan atau mesin fisik terhubung ke jaringan internet untuk mengkomunikasikan data tanpa memerlukan campur tangan manusia (Cloud Host, 2020). Karena luasnya aktivitas internet dan penyimpanan data di server, keamanan siber diperlukan untuk melindungi dari kejahatan digital seperti peretasan data pribadi, pencurian, penyalahgunaan, dan bahkan penipuan yang memanfaatkan data siapa pun.

Ancaman dunia maya yang terus berkembang, berkembang, dan berubah dengan cepat, pelanggaran seperti program yang dapat menyusup ke fasilitas sensitif pemerintah dan menyebabkan kerugian yang luas di banyak negara,

meningkatkan tingkat kesadaran, memerlukan peningkatan pengawasan, pelatihan, atau pengendalian, dan prosedur yang digunakan untuk meningkatkan keamanan perusahaan atau bahkan keamanan negara.

Menurut *Oxford Dictionary* (2018), ancaman siber adalah upaya yang berpotensi membahayakan untuk menghancurkan atau mengeksploitasi jaringan atau sistem komputer. Sedangkan menurut Secureworks (2017), ancaman siber adalah ancaman dari aktor atau musuh yang berupaya melakukan penetrasi secara ilegal untuk menyusup atau mencuri data dengan menggunakan taktik, metode, dan prosedur (TTP) yang terukur dan spesifik. Virus atau *malware* komputer, penyadapan, perusakan data, manipulasi data, dan berbagai jenis penipuan atau pelanggaran lainnya di dunia maya merupakan contoh ancaman siber.

Pasca penangkapan Gottfird Svartholm Warg (salah satu pendiri The Pirate Bay), kelompok aktivis hacker bernama Null Crew melancarkan serangan terhadap situs pemerintah Kamboja pada September 2012. Aksi tersebut juga menjadi simbol protes keras terhadap sensor internet. Menanggapi penahanan Warg, Kru Null menyusup ke berbagai situs pemerintah, termasuk tentara Kamboja, dan mengungkapkan materi sensitif. Mereka juga memulai perang cyber melawan Kamboja. Mereka berhasil mencuri dan membocorkan lebih dari 5.000 dokumen dari Departemen Luar Negeri Kamboja.

Setahun kemudian, pada bulan Januari 2013, peretas Indonesia yang dikenal sebagai "Hmei7" menyerang situs web Kepolisian Militer Nasional Kamboja. Situs web Mahkamah Agung juga telah dibobol, namun tidak ada lagi materi yang dirilis selain apa yang ditemukan selama penyelidikan (ASEAN

Youth Model Document Conferences: 3).

Ini bukan pertama kalinya hacker Indonesia berkelahi dengan hacker Malaysia. Berbagai 'perang' pun terjadi di antara keduanya. Tagar #OpAustralia muncul karena pemerintah Australia melakukan operasi penyadapan dan peretas Indonesia menyerang situs web negara tersebut. Dalam satu kasus, beredar cerita bahwa seseorang sengaja melakukannya saat memancing di air keruh, dan menurut penelusuran IP, itu berasal dari Malaysia.

Akibatnya, peretas dari Indonesia berbalik dan melancarkan serangan terhadap situs-situs Malaysia, yang mengakibatkan runtuhnya situs tersebut di Malaysia. Selain kesal dengan isu persaingan hacker, ternyata hacker Indonesia punya tujuan lain. Peristiwa ini dilatarbelakangi oleh kecerobohan Malaysia dalam mengklaim sejumlah barang dari Indonesia dan perlakuan kasar terhadap pekerja migran di negaranya. Serangan ini mengakibatkan berbagai kelompok peretas Malaysia memulai serangan balik, tindakan defacing dan spoofing, serta serangan DDoS dari kedua negara. Beberapa hari setelah konflik berakhir, kedua belah pihak tiba-tiba berhenti menyerang satu sama lain dan memutuskan untuk menunggu dan melihat.

Pada tahun 2014 Indonesia telah memiliki sekitar 12 juta aktivitas malware dengan 12 ribu kasus merupakan insiden website dan 3 ribu diantaranya berupa serangan siber terhadap situs pemerintah dengan domain .go.id. Indonesia menduduki peringkat ke 13 dengan isu siber tertinggi di dunia.

Tiga situs pemerintah Thailand diretas oleh peretas menggunakan alias 'Fallag Gassrini dan Dr.Lamouchi,' termasuk Universitas Mahasarakham dan

Rumah Sakit Lam Luk Ka. Ketiga situs tersebut tidak dapat diakses sejak Minggu 23 Agustus 2015 malam, karena peretas memasang gambar Rohingya di situs tersebut. Mereka juga memposting catatan yang mengatakan, "Situs web Anda telah diserang oleh Fallag Gassrini dan Dr. Lamouchi."

Tiga situs lagi diretas keesokan harinya, Senin, 24 Agustus 2015. Tiga di antaranya, milik provinsi Tak, Sing Buri, dan Sa Kaeo, tidak dapat diakses. Namun belum ada kepastian siapa peretasnya. Menurut Kementerian Informasi dan Teknologi Thailand, geng peretasan ini terkenal di seluruh dunia dan sering melakukan serangan menggunakan alat berbasis Linux.

Besarnya kejahatan siber telah menyebabkan seluruh pemerintahan di dunia merasa perlu untuk memperkuat keamanannya sendiri, terutama negara-negara di Asia Tenggara yang menghadapi berbagai bentuk ancaman siber. Serangan dunia maya berdampak di Vietnam. Akses tidak sah ditemukan pada sistem jaringan dua bandara terbesar di Vietnam dan maskapai penerbangan nasional, Vietnam Airlines, pada Juli 2016. Peretas melakukan aksinya dengan mengambil alih panel informasi penerbangan dan sistem suara di bandara Noi Bai di Hanoi dan Tan di Kota Ho Chi Minh. Bandara Son Nhat. Peretas dari kelompok peretas Tiongkok 1937CN tidak mampu melakukan serangan yang lebih mematikan karena pihak bandara dengan cepat mengambil tindakan mematikan jaringan internet; Akibatnya, pengumuman mengenai jadwal penerbangan penumpang harus dilakukan secara manual melalui pengeras suara (Blake, 2016).

Pada tahun yang sama, Filipina menjadi sasaran serangan yang mengekspos database pemilunya ke seluruh dunia. Kelompok peretas LulzSec Pilipinas

melakukan hal ini dengan merusak situs web *Commission on Elections* (Comelec) dan mengubah grafik yang tidak ada hubungannya dengan pemilihan umum. Para peretas tidak hanya mengambil informasi yang tersedia untuk umum, tetapi juga data pendaftaran pemilih dan database yang penting untuk fungsi situs web Comelec. (2006, Rappler) Meskipun serangan siber di Filipina berhasil diatasi oleh pemerintah Filipina, kejadian ini tidak boleh dianggap enteng.

Thailand tidak kebal terhadap serangan siber. Pada bulan Agustus 2016, hampir semua bank di Thailand mengalami serangan terhadap jaringan Anjungan Tunai Mandiri (ATM) mereka. Serangan siber ini mengakibatkan kerugian sekitar USD 350 ribu atau THB 12 juta dengan nilai tukar saat ini. Thailand bekerja sama dengan perusahaan yang berbasis di California, FireEye, untuk mendeteksi serangan cyber ini dan menemukan malware ATM baru dari Rusia. Virus yang dikenal dengan nama RIPPER ini menyebar dengan memasukkan kartu ATM yang dirancang khusus dengan chip yang berfungsi sebagai mekanisme otentikasi Lafevre (2016).

Indonesia juga mendapat serangan siber pada tahun 2017 dan mendapat kerugian bisnis dalam negeri sebesar USD 34 miliar, ditambah kerusakan reputasi jangka panjang, studi ini dilakukan oleh firma konsultasi riset Forest & Sullivan dengan mensurvei 1.300 bisnis dan perusahaan IT yang berada di wilayah Asia-Pasifik juga memperediksi total kerugian dari adanya serangan siber yaitu USD 1.745 triliun, atau 7 persen dari PDB saat ini di wilayah tersebut. Studi ini juga menemukan 22 persen dari perusahaan yang telah di survei di Indonesia melaporkan mereka memiliki pelanggaran keamanan, sementara 27 persen tidak

yakin jika mereka memilikinya karena keterbatasan data penilaian forensik. Masih banyak bentuk *cyber* lainnya seperti *cyber terrorism* yang dapat mengancam keamanan negara yang perlu diwaspadai.

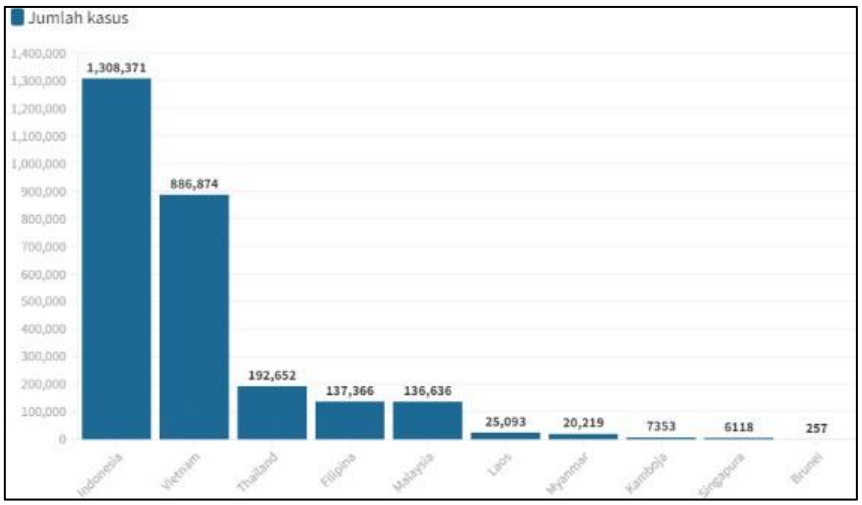
Di Singapura juga mengalami kasus sebanyak 1,5 juta yang terdaftar di perusahaan Singhealth Singapura dicuri pada bulan Juli 2018. Peretas menginflitrasi komputer SingHealth sebagai lembaga kesehatan terbesar di Singapura yang membawahi beberapa rumah sakit spesialis terbesar dan beberapa poli klinik. Peretas juga mencuri data pribadi pasien rawat jalan termasuk di dalamnya data Perdana Meneteri Singapura, Lee Hsien Loong.

Pada bulan Mei 2020, Tokopedia, sebuah pasar online Indonesia, mengalami serangan siber yang berujung pada pencurian data pengguna yang mencapai 91 juta. Peretas Whysodank menjual akun-akunyang bocor tersebut dengan harga Rp 74 juta. Terkait dengan pembayaran pennguna tokopedia dengan metode OVO, kartu kredit dan rekening dipastikan aman dan tidak dapat di retas oleh Whysodank.

Data yang terdapat dalam *Malware Infection Index* 2016 menunjukkan bahwa negara- negara ASEAN termasuk ke dalam jajaran negara yang rentan mengalami serangan *malware* di kawasan Asia Pasifik. Bahkan Indonesia mendapatkan peringkat kedua diantara negara ASEAN lainnya. Malware merupakan perangkat lunak yang dibuat untuk menyusup dan mencuri data yang pada komputer yang disusupinya. Malware merupakan salah satu bentuk cyber crime yang biasa digunakan untuk menyerang negara. Salah satu jenis *malware* yang banyak beredar dengan cara kerja mengambil alih perangkat komputer

sehingga pengguna perangkat komputer tersebut tidak dapat mengaksesnya disebut dengan *ransomware.* Pada saat menjalankan aksinya biasanya pengguna komputer tersebut diminta mengirimkan sejumlah uang untuk menebusnya (INTERPOL, 2020). Terdapat sekitar 2,7 juta *ransomware* yang terdeteksi di ASEAN selama tiga kuartal pertama tahun 2020 dalam data statistik yang dilaporkan oleh INTERPOL.

Gambar 1.1 Deteksi *ransomware* yang terdapat di negara- negara ASEAN pada Januari - September 2020



Sumber : INTERPOL 2020

Dalam data tersebut menunjukkan bahwa negara Indonesia paling banyak mendapatkan serangan siber dengan total kasus 1,3 Juta disusul dengan Vietnam, Thailand, Filipina, Malaysia, Laos, Myanmar, Kamboja, Singapore dan Brunei sebagai negara dengan kasus paling kecil di tahun itu.

Keamanan siber adalah perlindungan sumber daya data atau informasi

telematika dalam rangka mencegah kejahatan siber (Taru, 2019). Dari besarnya volume data pengguna internet kemungkinan besar akan memberikan peluang bagi penjahat dunia maya. Jika kita tidak menyadari hal ini dan tidak mempertimbangkan penggunaan keamanan siber untuk memerangi kejahatan internet, data kita akan menjadi sasaran kejahatan. Ini merupakan peringatan bagi seluruh negara, bukan hanya individu. Perubahan teknologi internasional berdampak pada pemanfaatan dunia maya yang mencakup seluruh elemen kehidupan berbangsa. Karena skala penggunaannya untuk mencuri informasi, menyebarkan ide-ide yang merusak, atau menyerang sistem informasi di berbagai industri, seperti data perbankan, jaringan militer, dan sistem pertahanan nasional, dunia maya dapat menjadi ancaman bagi suatu negara. Negara-negara Asia Tenggara sering menjadi sasaran serangan siber baik dari dalam maupun luar negeri. Kasus penggelapan dana bank, pornografi, pencurian data, hacking, dan carding misalnya, merupakan contoh *cybercrime* yang sering terjadi di masyarakat.

Cyber security merupakan respon pengamanan terhadap risiko dan ancaman modern yang dirasakan karena dampak adanya infromasi global atau biasa disebut dengan “internet” (Stevens, 2016). Dari banyaknya data dari yang telah mengakses internet akan memberikan peluang tersendiri bagi para pelaku kejahatan *cyber*. Ancaman – ancaman *cyber* yang sering terjadi baik yang berasal dari dalam maupun luar sehingga membuat negara - negara di kawasan Asia Tenggara semakin meningatkan keamanan *cyber* dalam level regional.

Bahaya siber ini, yang seringkali bersifat lintas batas negara, memerlukan

peningkatan kewaspadaan dan peningkatan keamanan siber, tidak hanya di tingkat nasional, namun juga di tingkat regional. Dengan maraknya berbagai kejahatan *cyber* tersebut, menarik perhatian tersendiri bagi ASEAN untuk mengatasinya. ASEAN memiliki suatu forum dalam bidang politik dan keamanan, yaitu ASEAN Regional Forum (ARF) yang dibentuk oleh ASEAN pada tahun 1994. Keberadaan ARF berfungsi untuk membahas terkait isu-isu politik dan keamanan di kawasan Asia Pasifik yang dibentuk sebagai dukungan proses integrasi dan pembangunan ASEAN *Political Security Community* (APSC). APSC merupakan bentuk keseriusan kerjasama antar negara-negara ASEAN untuk mengupayakan perdamaian dan keamanan serta kestabilan kawasan. Awal mula kerjasama APSC di deklarasikan di Bangkok pada 8 Agustus 1967 (Asean.org, 2017). Seiring perkembangan zaman APSC juga mulai berfokus pada isu non-tradisional salah satunya yaitu terkait ancaman *cyber*.

Meski kenyataannya APSC diharapkan mampu mewujudkan perdamaian di kawasan regional dan global. Ancaman dunia maya masih menjadi isu yang berkembang, terutama di kawasan Asia Tenggara. Dalam penelitian Lennon Chang yang bertajuk "*Cybercrime and Cyber Security in ASEAN*" menjelaskan bahwa pada tahun 2008, empat negara anggota ASEAN (Thailand, Vietnam, Singapura dan Filipina) termasuk dalam sepuluh negara dengan tingkat populasi kejahatan cyber tertinggi di kawasan Asia Pasifik. (Chang, 2017). *Malware Infection Index* tahun 2016 kemudian menunjukkan bahwa negara-negara ASEAN termasuk di kawasan Asia Pasifik yang rentan terhadap ancaman *malware*. Bahkan Indonesia berada di peringkat kedua setelah Pakistan, disusul Vietnam,

Filipina, dan Kamboja di peringkat kelima, masing-masing berada di peringkat keenam, dan ketujuh. Thailand, Malaysia, dan Singapura kemudian masing-masing menduduki peringkat ke-10, ke-11, dan ke-12 (Microsoft, 2016).

Dalam rangka mewujudkan keamanan nasional dan keamanan negara-negara ASEAN memiliki *regional organization* yang berfokus pada bidang cyber, ASEAN telah membentuk Regional Forum on *cyber security initiatives.* ARF *on cyber security initiatives* telah melaksanakan pertemuan pertamanya pada tahun 2006. Melalui forum regional ini, ASEAN mengharapkan adanya peningkatan kerjasama dalam penanganan ancaman *cyber*. Oleh karena itu, dibutuhkan penelitian lebih lanjut terkait hal ini untuk menjawab rumusan masalah.

Penelitian ini dilakukan dengan melakukan *review* terhadap penelitian-penelitian terdahulu. Penelitian terdahulu yang pertama merupakan karya dari Iqbal Ramadhan (2019) dengan judul Strategi Keamanan *Cyber Security* di Kawasan Asia Tenggara: *Self-help* atau Multilateralism?. Dalam penelitian ini disebutkan bahwa negara-negara Asia Tenggara dalam mengantisipasi ancaman cyber menggunakan strategi gabungan self-help versi neorealis dan kerjasama multilateral yang digunakan neoliberal institusionalis. Setiap negara perlu meningkatkan kekuatan teknologi, namun dalam mengatasi ancaman *cyber* yang bersifat dinamis dibutuhkan kerjasama multilateral yang terkoordinasi dengan baik sehingga dapat tercapai kepentingan bersama antar negara (Ramadhan, 2019).

Kedua yaitu karya M. Firly Fadila (2021) dengan judul Upaya ASEAN dalam meningkatkan cyber security di kawasan Asia Tenggara melalui ASEAN Regional

Forum on Cyber Security Initiatives. Upaya tersebut dapat dilihat melalui peran institusi internasional dalam liberalisme institusional yang menjadi indikator penelitian yaitu menyediakan aliran informasi dan kesempatan bernegosiasi, kemampuan membuat komitmen yang dapat dipercaya, dan memperkuat harapan tentang kesolidan dari kesepakatan internasional.

Terdapat kesamaan-kesamaan dari penelitian-penelitian terdahulu dalam menganalisa permasalahan *cyber security* di kawasan Asia Tenggara yaitu dengan menggunakan teori neorealisme. Sehingga penelitian ini berfokus pada strategi yang dilakukan oleh ASEAN melalui organisasi regional (ASEAN *Regional Forum on Cyber security Initiatives)* dalam menyikapi permasalahan di kawasan dengan menggunakan teori strategi dan konsep orgnasisasi regional.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, maka rumusan masalah dalam penelitian ini yaitu **"Bagaimana Strategi ASEAN regional forum *on cybersecurity initiatives* dalam menyikapi permasalahan *cybersecurity* di kawasan Asia Tenggara Tahun 2012 - 2021?"**

1.3 Tujuan Penelitian

Terdapat dua tujuan dalam penyusunan penelitian ini yaitu tujuan umum dan tujuan khusus sebagai berikut:

1.3.1 Tujuan Umum

Tujuan umum penelitian ini yaitu sebagai tugas akhir untuk memenuhi syarat dalam memperoleh gelar Sarjana Program Studi Hubungan Internasional

Fakultas Ilmu Sosial dan Ilmu Politik Universitas Pembangunan Nasional "Veteran" Jawa Timur.

1.3.2 Tujuan Khusus

Tujuan khusus penelitian ini yaitu untuk menganalisis dan menjelaskan Strategi ASEAN meningkatkan *cybersecurity* di kawasan asia tenggara melalui asean regional *forum on cyber security initiatives.*

1.4 Kerangka Pemikiran

Dalam penelitian ini, penulis menggunakan dua teori yaitu teori *cybersecurity,* strategi dan Regional Organization (*Cybersecurity Forum Initiative*) yang akan dijelaskan sebagai berikut :

1.4.1 Cybersecurity

Dunia saat ini berada pada era informasi yang merupakan tahap lanjutan dari era zaman dahulu, era pertanian, dan era industri. Di era informasi, keberadaan informasi mempunyai arti dan peranan yang sangat penting bagi seluruh aspek kehidupan, dan merupakan salah satu kebutuhan hidup bagi setiap orang, baik individu maupun organisasi, sehingga dapat dikatakan bahwa dalam masyarakat, informasi mempunyai peran yang sangat penting seperti aliran darah dalam tubuh, dimana sumber kehidupan bagi tubuh manusia (Anne, 1986).

Penemuan internet merupakan salah satu penemuan yang memberikan dampak terbesar terhadap informasi masyarakat. Kehadiran internet sebagai salah satu teknologi justru membuat manusia menjadi tidak kompeten, apapun arus komunikasi dan pengetahuannya. Internet telah mendorong seseorang untuk melakukan perubahan hidup yang signifikan. Internet layaknya teknologi lainnya,

bukannya tanpa batasan. Teknologi akan berdampak positif jika kita fokus pada kegunaan teknologi sesuai dengan nilai-nilai sosial masyarakat dan pribadi, serta adanya pembatasan oleh pemerintah untuk melindungi masyarakat dari dampak berbahaya yang akan ditimbulkannya (Nuriadin dan Harumike, 2021)

Kemajuan teknologi membawa dampak yang sangat besar bagi kehidupan manusia, baik positif maupun negatif. Evolusi ini tidak terlepas meberikan pengaruh pada konsep keamanan, karena manusia yang tidak lagi mendeteksi jarak dalam interaksi sosial dapat memiliki ancaman baru dari kejahatan dunia maya. Kejahatan dunia maya tidak hanya menyasar individu, namun juga menyasar organisasi bahkan dalam cakupan yang lebih besar yaitu negara. Oleh karena itu dengan banyaknya kasus mengenai serangan siber diperlukan penyesuaian yang tepat dalam pengembangan keamanan siber. Keamanan siber adalah seperangkat alat, kebijakan, konsep keamanan, upaya perlindungan keamanan, pedoman, teknik manajemen risiko, aktivitas, pelatihan, praktik terbaik, jaminan, dan teknologi yang dapat digunakan untuk menjaga lingkungan siber dan organisasi (Ardiyanti, 2014). Keamanan siber adalah upaya untuk menjamin pencapaian dan pemeliharaan properti keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan di lingkungan siber (Ardiyanti, 2014).

Penjelasan diatas membawa kita pada kesimpulan bahwa keamanan siber adalah upaya keamanan untuk menghindari dan merespons ancaman siber. Karena relevansi dari banyaknya isu keamanan siber di era saat ini, maka setiap negara mulai membangun keamanan siber, baik melalui peraturan internal maupun

kerjasama dengan negara lain. Dalam studi ini, salah satu aspek yang membatasi upaya ASEAN untuk diselidiki nanti adalah keamanan siber. Karena relevansi tantangan keamanan siber di era globalisasi, peneliti memilih topik ini untuk melakukan riset lebih lanjut.

1.4.2 Strategi

Untuk mencapai target dengan sesuatu yang terukur maka diperlukan adanya strategi. Setiap organisasi selalu memiliki sebuah rencana besar dan rencana tersebut dapat dicapai melalui langkah-langkah yang telah di sepakati bersama. Strategi menurut Coulter (2005) di definisikan sebagai suatu proses rencana atau tindakan – tindakan yang diarahkan pada tujuan organisasi di sesuaikan dengan peluang dan ancaman dalam lingkungannya. Sedangkan strategi menurut Griffin (2004) adalah rencana komperhensif untuk mencapai tujuan organisasi (*Strategy is acomrehensive plan for accomplishing an organization's goals*). Dari kedua definisi tersebut dapat disimpulkan bahwa strategi merupakan rencana khusus untuk mencapai tujuan organisasi yang disesuaikan dengan kondisi peluang dan ancaman di lingkungannya.

Strategi memiliki pernan penting dalam pencapaian tujuan suatu organisasi, karena startegi memberikan arah tindakan dan bagaimana tindakan tersebut harus dilakukan agar tujuan yang diinginkan dapat tercapai (Grant, 1999). Strategi sebagai pendukung untuk pengambilan keputusan. Strategi merupakan suatu bentuk pemersatuan antara keputusan-keputusan yang diambil oleh anggota organisasi lalu dijadikan acuan sesuai kesepakatan bersama. Strategi sebagai sarana koordinasi dan komunikasi. Salah satu peran penting strategi merupakan sarana koordinasi dan

memberikan kesamaan arah bagi anggota organisasi. Strategi merupakan target. Strategi yang telah disusun merupakan hasil dari penggabungan antara visi dan misi yang nantinya akan menentukan dimana organisasi tersebut dimsa yang akan datang. Dengan demikian strategi dapat menjadi target suatu organisasi.

1.4.3 Regional Organization

Kita hidup di dunia yang terdiri dari beberapa wilayah (Katzenstein 2005). Setelah peristiwa perang dunia kedua, regionalisme telah menyebar ke seluruh dunia dalam beberapa gelombang (Mansfield dkk. 1999; Söderbaum 2016; Väyrynen 2003). Perang, peralihan kekuasaan, globalisasi ekonomi dan penyebaran ide-ide baru tentang tatanan politik telah menyebabkan kemunculan dan pertumbuhan ruang trans dan supranasional serta permintaan akan ruang baru bentuk pemerintahan di luar negara-bangsa (Buzan dan Wæver 2010; Lake dan Morgan 1997; Tel 2014a; Wunderlich 2007: 45–47). Salah satu yang paling luas jangkauannya dengan adanya perkembangan ini adalah menjamurnya organisasi-organisasi regional. Sebagai organisasi-organisasi yang ada telah bertambah keanggotaannya dan organisasi-organisasi baru telah dibentuk, saat ini hampir tidak ada satu negara pun di dunia yang tidak menjadi anggota setidaknya satu regional organisasi. Namun, selain peningkatan jumlah dan cakupan geografis, organisasi-organisasi regional juga telah mengambil tugas-tugas baru dan mengambil alih wewenang yang lebih besar hubungannya dengan negara-negara anggotanya (Acharya 2014: 84–93; Börzel dan Risse 2016).

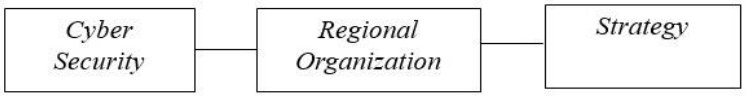
Permasalahan yang umum terjadi di berbagai wilayah adalah memastikan bahwa keamanan siber dipandang sebagai isu kebijakan, dan adanya kesadaran

yang memadai di kalangan pembuat kebijakan dan pemimpin politik akan bahayanya jika mengabaikan risiko siber. Di beberapa daerah masih ada persepsi bahwa keamanan siber adalah masalah teknis, bukan masalah kebijakan. Semua pembicara sepakat bahwa keamanan siber tidak bisa diserahkan hanya kepada para ahli teknis. Para pengambil kebijakan mempunyai tanggung jawab untuk memastikan perlindungan terhadap infrastruktur penting, mencegah kejahatan siber dan tindakan jahat, serta menumbuhkan suasana yang kondusif bagi pertumbuhan ekonomi—sehingga harus mengambil peran aktif dalam keamanan siber.

Karena kejahatan siber dan operasi siber bersifat transnasional, respons yang efektif memerlukan kerja sama untuk mengadili kejahatan dan mengatasi tindakan jahat, ofensif, atau agresif. Pertukaran sumber daya dan informasi antar negara dan antar wilayah dapat meningkatkan efisiensi penegakan hukum dan atribusi. Kolaborasi dan berbagi informasi, khususnya berbagi kebijakan atau doktrin siber dengan pihak lain untuk memperjelas niat, juga ditekankan sebagai CBM regional yang berharga. Terakhir, kolaborasi ini dapat dimanfaatkan untuk mendorong peningkatan kapasitas. Salah satu pembicara mengusulkan agar organisasi regional dapat membentuk ‘tim bantuan siber’ yang akan bekerja dengan anggota yang masih mengembangkan kemampuan mereka untuk mengatasi permasalahan di luar perbatasan negara mereka.

1.5 Sintesa Pemikiran

Gambar 1. 2 Sintesa Pemikiran



Berdasarkan gambar diatas dapat dijelaskan bahwa sintesa pemikiran yang dihasilkan dari teori cybersecurity sebagai bentuk isu keamanan kontemporer yang menjadi perhatian tidak hanya bagi negara tetapi juga menjadi isu badan regional memerlukan strategi untuk menjawab berbagai permasalahan yang muncul terkait dengan keamanan siber. Strategi dapat muncul berupa kebijakan, baik secara domestik maupun internasional melalui adanya organisasi regional, dalam hal ini penulis berfokus pada peran lembaga regional yang menaungi negara-negara di kawasan Asia Tenggara. Organisasi regional pada penelitian ini menjadi objek analisis terkait dengan bagaimana upaya mereka umtuk mewujudkan keamanan siber bagi negara-negara anggota melalui strategi yang telah mereka bangun serta bagaimana strategi tersebut diimplementasikan.

1.6 Argumen Utama

ASEAN Regional Forum sebagai organisasi regional di kawasan Asia Tenggara memiliki kapabilitas untuk menciptakan strategi dalam upaya meningkatkan *cybersecurity* di kawasan tersebut. Sejak 2006 hingga 2012, ARF telah melakukan berbagai pertemuan yang pada akhirnya berhasil menciptakan strategi terkait dengan *cybersecurity*. Keberhasilan ARF muncul pada tahun 2012

yang menghasilkan. ARF *on Cybersecurity Forum Initiatives*. Terdapat 5 poin strategi yang dihasilkan pada forum tersebut. Kelima strategi tersebut berupa:

(1) *promote further consideration*;

(2) *Promote dialogue on confidence-building, stability, and risk reduction;*

(3) *Encourage and enhance cooperation;*

(4) *Develop an ARF work plan on security in the use of ICTs;*

(5) *Review a possibility to elaborate the sphere of the use of ICTs.*

Analisis penelitian ini kemudian akan berusaha menjawab bagaimana implementasi dari kelima poin strategi tersebut secara mendalam melalui rapat, forum, diskusi, dan segala bentuk tindakan lain yang diambil oleh ASEAN terkait dengan upaya mereka menerapkan lima poin strategi tersebut.

1.7 Metode Penelitian

Dalam metode penelitian ini dibagi menjadi lima bagian yaitu tipe penelitian, jangkauan penelitian, teknik pengumpulan data, teknik analisis data dan sistematika penulisan yang akan dijelaskan sebagai berikut:

1.7.1 Tipe Penelitian

Peneliti menggunakan tipe penelitian deskriptif. Penelitian deskriptif mempunyai pernyataan yang jelas terkait permasalahan dan informasi detail yang dibutuhkan (Malhotra, 2007). Dalam penelitian ini penelitian deskriptif digunakan untuk mendapatkan pengetahuan mengenai strategi ASEAN dalam meningkatkan cyber security di kawasan Asia Tenggara melalui ASEAN Regional Forum on cybersecurity initiatives.

1.7.2 Jangkauan Penelitian

Untuk membatasi jangkauan penelitian, peneliti memilih jangka waktu selama 9 tahun tahun terhitung sejak tahun 2012 hingga 2021. Tahun 2012 dipilih karena pada tahun tersebut terdapat pertemuan – pertemuan dari implementasi dari strategi ARF *on cybersecurity forum initiative*. Penelitian dibatasi hingga tahun 2021 dimana tahun tersebut menjadi tahun terakhir implementasi strategi yang dilakukan oleh ARF *on cybersecurity forum initiative* dan dilanjutkan dengan program baru.

1.7.3 Teknik Pengumpulan data

Strategi pengumpulan data dapat digunakan dengan data primer atau sekunder. Data primer adalah informasi yang diperoleh langsung dari wawancara atau observasi, sedangkan data sekunder adalah informasi yang sudah ada. Peneliti menggunakan data sekunder yang sebelumnya dapat diakses dalam penelitian ini, yang mungkin berasal dari sumber bekas seperti buku, jurnal, dokumen di website, laporan, dan sebagainya yang terkait dengan permasalahan yang diteliti (Sugiyono, 2012).

1.7.4 Teknik Analisis Data

Ada dua macam pendekatan analisis data: kuantitatif dan kualitatif. Analisis data kuantitatif dilakukan dengan memusatkan perhatian pada data numerik atau angka, yang kemudian diolah secara statistik. Sedangkan analisis data kualitatif dilakukan dengan menggunakan penalaran berdasarkan kejadian-kejadian yang dapat diamati, sehingga menghasilkan kesimpulan deduktif atau induktif yang tidak dapat dicapai di laboratorium. Penelitian kualitatif menurut Abdussamad (2002) menghasilkan data tekstual mengenai peristiwa yang dilihat.

Penelitian kualitatif menurut Saryono adalah “penelitian yang bertujuan untuk mempelajari, mengeksplorasi, mendeskripsikan, dan menjelaskan nilai-nilai atau ciri-ciri fenomena sosial yang tidak dapat dievaluasi atau dipahami secara kuantitatif” (Saryono, 2007).

Teknik analisis data yang optimal untuk penelitian ini adalah kualitatif karena peristiwa yang diberikan bersifat alamiah dan dapat diperiksa dengan memperhatikan tingkah laku partisipan yang diamati sehingga menghasilkan kesimpulan yang bersifat deduktif atau induktif. Teknik analisis ini, menurut Miles dan Huberman (1994), akan dilakukan dengan melakukan tiga aliran kegiatan analisis kualitatif yang tercantum di bawah ini: Reduksi data adalah proses mengidentifikasi data mana yang dapat diambil dan dimusnahkan dengan cara memilih, memfokuskan, menyederhanakan, dan memodifikasi data. Proses ini akan diulang sampai pencarian selesai. Penyajian data, atau proses penyajian informasi yang dikumpulkan secara lugas dan mudah dipahami, dapat berbentuk ringkasan singkat, grafik, atau sejenisnya: menarik kesimpulan dan memverifikasi, khususnya menyajikan fakta-fakta penting yang ditemukan selama proses penelitian. Hasil yang diperoleh mungkin memberikan atau tidak memberikan solusi yang jelas terhadap rumusan masalah.

1.7.5 Sistematika Penulisan

Sistematika penulisan penelitian dipisahkan menjadi empat bab yang disusun secara logis untuk membantu pembaca memahami alur penelitian ini. Pembagiannya dilakukan sebagai berikut:

Bab 1 : Pendahuluan. Bab ini akan memuat bagian-bagian sebagai berikut: latar

belakang, rumusan masalah, tujuan penelitian, keunggulan penelitian, kerangka pemikiran, argumentasi utama, metode penelitian, dan sistematika penulisan.

Bab 2 : Strategi. Pada bab ini akan memuat pemaparan strategi ARF on cybersecurity forum initaitve poin pertama, kedua dan ketiga beserta implementasinya.

Bab 3: **Strategi**. Pada bab ini akan berisi tentang pemaparan strategi keempat dan kelima beserta implementasinya.

Bab 4 : Kesimpulan. Bab ini merupakan bab penutup yang berisi kesimpulan mengenai teknik yang diterapkan berdasarkan rumusan tantangan yang dihadapi, serta gagasan untuk penelitian selanjutnya.