BAB I

PENDAHULUAN

I.1 Latar Belakang Masalah

Perkembangan teknologi dalam beberapa dekade terakhir mulai mendatangkan berbagai tantangan yang belum pernah dihadapi oleh negara dan organisasi internasional manapun di dunia ini. Banyak isu dan masalah baru yang muncul dari perkembangan teknologi yang semakin pesat. Beberapa masalah tersebut adalah pencurian hak paten antar perusahaan teknologi, kegiatan pencurian data nasabah bank, kegiatan *hacking* yang dapat memicu ketegangan antar negara, penipuan jual-beli *online*, *hoax* yang semakin hari semakin bertambah serta persoalan lain di dunia maya yang saat ini menjadi perhatian masyarakat dunia.

Salah satu pengaruh akan hal ini adalah hal yang disebut dengan *cyber insecurity*, atau yang secara harfiah dapat diterjemahkan sebagai ketidakamanan dunia maya. Dunia maya telah berubah secara signifikan dalam beberapa tahun ini menjadi semakin membahayakan, hal ini terjadi karena terlalu banyak kekuatan yang terkonsentrasi di tangan segelintir orang atau organisasi (Dickson, 2018). Pada masa awal dunia maya, mayoritas individu diberdayakan yang mana sangat berbeda dengan beberapa tahun terakhir dimana pemerintah, perusahaan, bahkan kriminal teroganisir memegang keseimbangan kekuasaan mengenai segala hal yang ada di dunia maya dengan caranya masing-masing, hal inilah yang mendorong semua orang menjadi lebih peduli mengenai *cybersecurity* atau keamanan siber.

Pada awal munculnya internet, *cybersecurity* bahkan tidak ada dalam radar kebanyakan perusahaan, negara dan organisasi internasional. Selama beberapa

tahun terakhir setelah banyak kegagalan dan krisis yang berdampak pada dunia dari setiap ukuran dan ruang lingkup, *cybersecurity* terus meningkat sebagai prioritas dan muncul sebagai aspek integral dari tugas dewan direksi dan pengawasan kepada perusahaan yang diawasinya. Dynkin (2018) menyatakan bahwa *cyberthreats* yang terus berevolusi, berkembang, dan berubah membuat manajemen dibanjiri dengan panduan tentang pengawasan, pelatihan, dan sejumlah kontrol teknis dan prosedural yang diperlukan untuk meningkatkan postur keamanan perusahaan atau bahkan negara. Selain laju cepat evolusi dalam *cybersecurity*, tren baru-baru ini dari pelanggaran tinggi membuat semua orang beralih pada siaga tinggi untuk ancaman yang sangat spesifik, seperti program yang dapat menyusup ke fasilitas sensitif pemerintah atau bahkan program yang dapat merugikan banyak negara sekaligus dalam skala besar.

Sementara pemahaman tentang kontrol teknis dan risiko spesifik merupakan bagian utama dari program *cybersecurity* apa pun, penting untuk memahami bahwa ada prinsip yang wajib dipahami yaitu bahwa *cybersecurity* bukanlah negara biner (aman atau tidak aman), tetapi lebih bersifat kontinyu, proses yang berulang dan dinamis. Hal ini membuat semua pihak baik negara, organisasi internasional dan perusahaan harus memiliki kesempatan untuk memajukan pengetahuan secara berarti, dan mengembangkan konsepsi yang lebih jelas tentang sifat *cybersecurity*, tujuan program *cybersecurity* yang dinamis, dan metodologi yang harus diterapkan untuk mencapai keamanan dunia maya yang reliabel dalam menghadapi *cyber threat*.

Cyber threat sendiri menurut Oxford Dictionary (2018) adalah

Kemungkinan upaya jahat untuk merusak atau mengganggu jaringan atau sistem komputer. Sedangkan menurut Secureworks (2017) *cyber threat* adalah ancaman aktor atau musuh yang mencoba mendapatkan akses ke sistem untuk mengakses file dan menyusup atau mencuri data dengan Taktik, Teknik dan Prosedur (TTP) yang digunakan secara terukur dan spesifik. *Cyber threat* dapat berupa virus komputer, pencurian hak kekayaan intelektual, pencurian uang, manipulasi data, penghancuran data, penyadapan melalui gawai, dan kecurangan atau pelanggaran di dunia maya lainnya.

Cyber threat menjadi sesuatu yang ditakuti di seluruh dunia, tidak terkecuali negara-negara Asia Tenggara yang pernah merasakan masifnya kejahatan di dunia maya. Vietnam pernah merasakan bagaimana serangan siber berdampak cukup masif dan merepotkan banyak pihak. Pada 29 Juli 2016, Peretas berhasil melakukan serangan terhadap dua bandara terbesar Vietnam dan maskapai penerbangan nasional, Vietnam Airlines. Para peretas membajak layar informasi penerbangan dan sistem suara di dalam bandara Noi Bai di Hanoi dan Tan Son Nhat di Ho Chi Minh City. Peretas yang diyakini dari kelompok peretas di China bernama 1937CN gagal melakukan serangan yang lebih fatal karena pihak bandara langsung mematikan jaringan internet, namun sebagai konsekuensinya pengumuman penerbangan dan jadwal penerbangan diberitahukan kepada penumpang secara manual menggunakan pengeras suara. (Blake, 2016)

Sebelumnya di tahun yang sama, Filipina juga mengalami serangan peretas yang menjadikan *database* pemilihan umum dapat diakses oleh seluruh dunia. Grup peretas LulzSec Pilipinas mengacak-acak *website* Commission on Elections

(Comelec) dan mengganti dengan gambar-gambar yang tidak ada kaitannya dengan pemilihan umum. Paparan data yang dicuri dari *website* Comelec tidak hanya mencakup informasi yang tersedia untuk umum, tetapi juga data pemilih, data pendaftaran pemilih, dan basis data yang relevan dengan fungsionalitas *website* Comelec. (Rappler, 2016) Meski pemerintah Filipina dapat menyelesaikan permasalahan ini, pemilihan umum 2016 di Filipina merupakan bukti nyata bahwa *cyber threat* tidak bisa dianggap remeh.

Negara selanjutnya yang terkena serangan siber adalah Thailand. Pada tanggal 31 Agustus 2016 hampir seluruh bank di Thailand menerima serangan pada jaringan anjungan tunai mandiri (ATM) yang tersebar di seluruh Thailand. Kerugian yang ditimbulkan oleh serangan peretas ini sekitar USD 350 ribu atau THB 12 juta pada kurs saat itu. Thailand bekerjasama dengan perusahaan asal California, FireEye, dan menemukan bahwa mereka telah mendeteksi sampel virus ATM baru dari Rusia yang mungkin terkait dengan serangan Thailand. Virus ini bernama RIPPER dan berinteraksi dengan ATM dengan memasukkan kartu ATM yang dibuat khusus dengan chip yang berfungsi sebagai mekanisme otentikasi. (Lefevre, 2016)

Indonesia juga tidak luput dari serangan dunia maya. Menurut laporan Microsoft, Serangan siber pada perusahaan Indonesia pada tahun 2017 merugikan bisnis dalam negeri sebesar USD 34 miliar karena kerugian keuangan langsung dan kerusakan reputasi jangka panjang, Studi ini dilakukan oleh firma konsultasi riset Frost & Sullivan dengan mensurvei 1.300 bisnis dan perusahaan IT di Wilayah Asia-Pasifik juga menempatkan total potensi kerugian ke wilayah itu dari serangan

siber di USD 1.745 triliun, atau 7 persen dari PDB saat ini di wilayah itu. Hampir separuh dari perusahaan Indonesia mungkin telah terpengaruh oleh serangan siber tahun lalu. Studi ini menemukan 22 persen dari perusahaan yang disurvei di Indonesia melaporkan mereka memiliki pelanggaran keamanan, sementara 27 persen tidak yakin jika mereka memilikinya, karena kurangnya data penilaian forensik. Mirisnya, 51 persen organisasi tidak berpikir tentang *cybersecurity* sama sekali. (Woolgar, 2018)

Masifnya kerugian akibat serangan siber dan kurangnya pengetahuan negara dan perusahaan membuat berbagai pihak merasa perlunya ada kerjasama yang dapat menjadikan iklim perdagangan di kawasan Asia Tenggara menjadi aman dari serangan peretas. Saat ini masing-masing negara yang ada di kawasan Asia Tenggara dan organisasi internasional khususnya organisasi pemerintah internasional seperti Association of Southeast Asian Nations (ASEAN) bersama-sama mencari solusi dari permasalahan *cybersecurity*. Guna menanggulangi berbagai masalah tersebut, ASEAN mulai menginisiasi program yang bernama ASEAN Cyber Capacity Program (ACCP).

Pada mulanya, kebijakan keamanan siber dan teknologi ASEAN sering berfungsi sebagai sarana untuk menumbuhkan blok ekonomi melalui *e-Commerce,* mengingat pada awalnya ASEAN adalah organisasi pemerintah internasional berbasis ekonomi. e-ASEAN Framework 2000 yang digagas pada 25 November 2000 bertujuan untuk menumbuhkan perdagangan elektronik, meliberalisasi perdagangan produk dan layanan Teknologi Informasi dan Komputer (TIK) dengan fokus pada pembangunan infrastruktur TIK di negara-negara anggota yang kurang

berkembang dan memperkuat layanan *e-Government* di negara-negara anggota yang maju. *Framework* ini memiliki tujuan ambisius untuk digitalisasi ekonomi dan pemerintah, tetapi pada saat itu tidak memiliki diskusi yang memadai tentang ranah keamanan siber (*cybersecurity*) (Secretariat, 2011).

Program lanjutan dari e-ASEAN Framework 2000 adalah Telecommunications and IT Ministers Meeting (TELMIN) yang pertama kali dilaksanakan pada 14 Juli 2001 di Malaysia tanpa ada *concern* terhadap *cybersecurity*. *Cybersecurity* baru mendapatkan perhatian pada saat TELMIN ke-3, pada 13 September 2003 di Singapura. Pertemuan ini pertama kali menyatakan bahwa *cybersecurity* adalah suatu keniscayaan dan tidak dapat diabaikan begitu saja. Pertemuan ini menyimpulkan bahwa setiap negara anggota harus membentuk Computer Emergency Response Team (CERT) sendiri pada tahun 2005. Meskipun tujuan ini tidak selesai tepat waktu, saat ini semua negara anggota ASEAN memiliki CERT mereka masing-masing (Learning, 2015).

Puncaknya adalah pertemuan ASEAN Ministerial Conference on Cybersecurity (AMCC) di Singapura pada 11 Oktober 2016 yang bertujuan untuk meningkatkan kapasitas ASEAN dalam mengatasi ancaman siber yang semakin lama semakin banyak terjadi di kawasan ASEAN (Parameswaran, Singapore Unveils New ASEAN Cyber Initiative, 2016). Negara-negara anggota ASEAN menyerukan kerjasama *cybersecurity* yang lebih dekat, koordinasi yang lebih kuat dari sekadar inisiatif pengembangan kapasitas *cybersecurity* regional, dan memperkuat diskusi dengan fokus khusus pada *cybersecurity*. Sebagai bagian dari strategi keamanan siber, ASEAN mengakui kenyataan bahwa semakin lama

negara-negara menjadi lebih saling terkait, hal itu juga meningkatkan kemungkinan bahwa dampak *cybercrime* dapat meluas ke negara-negara lain di dalam regional ASEAN. Sehingga pada ASEAN Summit ke-32, 28 April 2018 di Singapura ASEAN Cybersecurity Cooperation resmi dibentuk sebagai lanjutan program ASEAN Cyber Capacity Program. (Yinglun, 2018)

ASEAN Cyber Capacity Program dibentuk karena negara-negara anggota ASEAN mengakui perlunya mempertahankan dunia maya dan infrastruktur teknologi informasi mereka. Untuk itu, ada empat mekanisme ASEAN yang melihat ke aspek *cybersecurity* dan *cybercrime*, yaitu: the ASEAN Ministerial Meeting on Transnational Crime (AMMTC); ASEAN Telecommunications and IT Ministers Meeting (TELMIN); the ASEAN Regional Forum (ARF), dan the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC). AMMTC meninjau isu-isu regional dan menetapkan agenda untuk berbagai lembaga pemerintah Asia Tenggara untuk bekerja sama dalam bidang kejahatan transnasional, termasuk *cybercrime*. SOMTC kemudian melaksanakan agenda AMMTC. SOMTC telah mengidentifikasi delapan wilayah kejahatan transnasional, termasuk *cybercrime*, ada di bawah wewenangnya. Program-program ARF termasuk seminar-seminar ASEAN tentang terorisme *cyber*, konferensi tentang terorisme dan Internet, lokakarya tentang respon insiden *cyber* dan langkah-langkah kesiapsiagaan untuk meningkatkan *cybersecurity* (Putra, 2018).

ASEAN Cyber Capacity Program (ACCP) bertujuan untuk mendanai sumber daya, menambah keahlian dan pelatihan untuk membantu negara-negara

ASEAN membangun infrastruktur mereka yang diperlukan untuk melawan ancaman dunia maya. Hal ini akan mencakup berbagai mekanisme termasuk lokakarya, seminar dan konferensi, usaha konsultasi untuk membentuk undang-undang dan strategi keamanan siber untuk semua negara di bawah naungan ASEAN. Program ini menargetkan pejabat kebijakan, diplomat, jaksa, serta operator teknis dan analis dari seluruh negara ASEAN. Pelatih program ini dipilih dari Pusat Global Inovasi INTERPOL di Singapura, Mitra Dialog ASEAN, akademisi dari Centre of Excellence for National Security (CENS) di S. Rajaratnam School of International Studies (RSIS), agen keamanan siber di Singapura dan agensi terkait lainnya. Acara akan dipublikasikan melalui berbagai mekanisme ASEAN dan perwakilan dari Negara Anggota ASEAN akan diundang untuk mendaftar yang nantinya semua akan tercakup dalam ASEAN Cybersecurity Cooperation Strategy. (CSA, 2016)

Peristiwa tahunan yang akan dimasukkan dalam kalender ACCP adalah Pekan Internasional Singapura, yang menggabungkan Konferensi Tingkat Menteri ASEAN tentang Keamanan Dunia Maya sebagai platform utama untuk pembahasan kebijakan dan strategi keamanan siber regional. Acara lain adalah Lokakarya Cybersecurity yang diselenggarakan bersama oleh Singapura dan Amerika Serikat dengan partisipasi dari negara lain serta mitra industri. Singapura sebagai negara yang memiliki iklim dunia siber yang paling baik di ASEAN akan menginvestasikan SGD 2 juta pada 2017 dalam inisiatif selama lima tahun, sehingga totalnya menjadi SGD 10 juta. Singapura juga mempromosikan CyberGreen, Prakarsa global yang bertujuan untuk menilai dan mempromosikan

kesadaran tentang kesehatan dunia maya dan potensi kerentanan di negara-negara, serta kebutuhan ASEAN untuk memulai dialognya sendiri mengenai norma-norma dunia maya dalam *platform* yang sama seperti United Nations Group of Government Experts (UNGGE) (CyberGreen, 2018).

Pengamanan jaringan dan dunia maya di kawasan ASEAN menjadi sangat penting dan mendesak. Hal ini terkait dengan masifnya pertumbuhan dunia digital. Dalam beberapa tahun terakhir, Asia Tenggara telah menjadi sarang pertumbuhan dan inovasi digital, sebagian besar karena konektivitas internet yang lebih baik dan adopsi ponsel cerdas. Potensi ekonomi internet di kawasan Asia Tenggara diprediksi akan mencapai $ 200 miliar pada 2025. (Choudhury, 2017) Karena semakin banyak orang terhubung ke internet, ancaman keamanan dunia maya juga meningkat. Ancaman tersebut menjadi lebih kompleks di lapangan dan membutuhkan upaya yang lebih besar dari berbagai pemangku kepentingan untuk mengatasinya.

I.2 Rumusan Masalah

Mencermati perdebatan mengenai keefektifan ASEAN Cybersecurity Cooperation Strategy dalam menghadapi ancaman siber di Asia Tenggara, penulis tertarik untuk meneliti secara lebih obyektif, Bagaimanakah prospek implementasi ASEAN Cybersecurity Cooperation Strategy beroperasi dalam menghadapi ancaman keamanan siber di Asia Tenggara?

I.3 Tujuan Penelitian

Penelitian ini memiliki tujuan untuk menjelaskan dan menganalisis sejauh mana prospek implementasi ASEAN Cybersecurity Cooperation Strategy dalam menjaga stabilitas keamanan, ekonomi dan politik di Asia Tenggara dengan cara menyepakati terbentuknya ASEAN Cybersecurity Cooperation Strategy yang bertugas untuk mengamankan negara-negara di Asia Tenggara dari ancaman keamanan siber. Selain itu, penelitian ini juga bertujuan untuk melihat apa saja permasalahan mendasar mengenai keamanan siber yang dihadapi oleh organisasi internasional seperti ASEAN dan negara-negara yang menjadi anggotanya.

I.4 Teknik Pengumpulan Data

Penelitian ini disusun dengan menggunakan teknik pengumpulan data sekunder. Data sekunder didapatkan melalui studi pustaka dengan menulusuri berbagai sumber pustaka yang memiliki keterkaitan dengan kepentingan penelitian. Seperti artikel jurnal, buku, koran, majalah, dokumen negara, laporan organisasi, laporan penelitian, video, dan website.

I.5 Ruang Lingkup Penelitian

Fokus pengamatan dalam penelitian ini adalah tata kelola teknologi yang diimplementasikan oleh ASEAN untuk mengurangi kesenjangan teknologi yang ada di negara-negara Asia Tenggara, serta faktor-faktor yang mempengaruhi terbentuknya ASEAN Cyber Capacity Program dan ASEAN Cybersecurity Cooperation Strategy yang bertujuan untuk menjadikan negara-negara tersebut

memiliki kemampuan yang setara dalam menghadapi ancaman keamanan siber.

I.6 Jenis Penelitian

Jenis penelitian yang digunakan adalah deskriptif dengan melihat realitas sosial dan gambaran yang lebih detail melalui kajian konseptual yang disusun. Penelitian ini mendeskripsikan faktor-faktor apa sajakah yang melatarbelakangi ASEAN Cybersecurity Cooperation Strategy dan bagaimana ASEAN Cybersecurity Cooperation Strategy beroperasi.

I.7 Sistematika Pembahasan

Pada bab kedua, penulis menyertakan kerangka pemikiran penelitian, dilanjutkan bab ketiga membahas mengenai ASEAN Cybersecurity Cooperation sebagai wujud kerjasama internasional melalui mekanisme IGO. Pada bab keempat penulis menjelaskan bagaimana kesenjangan teknologi informasi di negara-negara yang menjadi anggota ASEAN. Pada bab kelima, akan membahas bagaimana prioritas keamanan siber dan tren tata kelola teknologi informasi di lingkungan regional ASEAN. Bab keenam merupakan kesimpulan dan saran oleh penulis.