# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang Masalah

Teknologi merupakan suatu aspek yang terlalu sulit untuk dibendung dalam suatu peradaban manusia dimana semua orang memerlukan sesuatu serta solusi dalam setiap permasalahan yang dengan mencari setiap alternatif disemua bidang kehidupan. Fleksibel menjadi perumpamaan yang tepat untuk menggambarkan sesuatu yang memiliki arus kencang dan dinamis tanpa batas, begitu pula kajian ilmu hubungan internasional yang memiliki sifat multidisipliner yaitu mempelajari berbagai macam ilmu pengetahuan yang ada hingga lingkup kajian nya pun berada diluar batas negara, baik dalam segi territorial maupun sosial politik ekonomi.

Dalam satu dekade terakhir, perkembangan teknologi informasi dan komunikasi (TIK) telah memberikan kontribusi positif terhadap pertumbuhan ekonomi global dan telah dikaitkan dengan peningkatan produktivitas, daya saing, dan keterlibatan masyarakat (Setiadi, Sucahyo, & Hasibuan, 2012). Namun, karena lembaga pemerintah, bisnis, dan masyarakat semakin terhubung di dunia maya, tantangan baru yang ditimbulkan oleh ancaman siber membutuhkan lebih banyak perhatian untuk mengembangkan keamanan siber yang kuat (Anjani, 2021).

Kajian Hubungan Internasional selalu bergerak pada dimensi yang dinamis dan selalu mengalami pembaharuan dengan peradaban yang dipengaruhi teknologi, dengan semua perkembangan teknologi yang ada mulai dari teknologi yang berelasi langsung dengan kehidupan sehari hari seperti berbelanja online, komunikasi jarak

jauh, hingga pengamanan data privasi hampir semua sudah bersinggungan langsung dengan adanya teknologi dan mengejar ketertinggalan dari peradaban sebelumnya dengan hakekat manusia atau individu yang selalu ingin menemukan solusi disetiap permasalahan.

Konsep dari Internet of Things (IoT) melibatkan 3 elemen utama, yaitu: objek fisik atau nyata yang telah diintegrasikan ke dalam modul sensor, koneksi internet, dan pusat data di server untuk menyimpan data atau informasi dari aplikasi. Penggunaan objek yang terhubung ke internet akan mengumpulkan data yang kemudian diolah menjadi "big data" yang kemudian diproses dan dianalisis oleh lembaga pemerintah, perusahaan terkait, dan lembaga lainnya, dan kemudian digunakan untuk kepentingan masing-masing (Triwahyuni, 2020).

Pada lingkup internasional, semua interaksi didalam nya sudah tersentuh secara menyeluruh oleh teknologi mulai dari cara komunikasi publik, negosiasi, kerjasama bilateral maupun multilateral untuk suatu kepentingan yang ingin dicapai sudah jarang melakukan hal tersebut dengan cara tradisional. Cara modern dianggap lebih efisien baik dalam hal waktu, anggaran dan lainnya sehingga cara tradisional sudah mulai ditinggalkan dan beralih ke hal yang berteknologi seperti mengirimkan pesan diplomatis, undangan diplomatis oleh pejabat suatu negara ke negara lain bahkan hingga konferensi negara-negara sudah bisa dilakukan secara daring hasil dari akibat adanya pandemi beberapa waktu lalu dan berlangsung hampir diseluruh belahan dunia memaksa semua hal untuk berimprovisasi agar semua tetap berjalan sebagaimana mestinya.

Di era digital saat ini, ancaman keamanan siber semakin kompleks dan beragam. Setiap hari kita menggunakan teknologi digital seperti smartphone, komputer, internet, dan perangkat Internet of Things atau yang biasa disebut IoT, sehingga kita menjadi semakin rentan terhadap serangan siber. Ransomware, sebuah jenis perangkat lunak berbahaya yang menginfeksi komputer dan perangkat seluler, telah menyebar dengan cepat di seluruh dunia dan menjadi salah satu metode serangan favorit oleh para penjahat siber. Ransomware membatasi akses pengguna ke berkas mereka dan sering kali mengancam untuk menghancurkan data secara permanen kecuali tebusan dibayarkan.

Menurut sebuah laporan Cybersecurity Ventures pada tahun 2017, perkiraan kerugian akibat serangan *ransomware* mencapai $5 miliar di seluruh dunia pada tahun tersebut. Jumlah ini mengalami peningkatan drastis dibandingkan dengan $325 juta pada tahun 2015, meningkat sebanyak 15 kali lipat hanya dalam dua tahun. Proyeksi kerugian untuk tahun 2018 mencapai $8 miliar, yang kemudian meningkat lagi menjadi $11,5 miliar pada tahun 2019 (Ventures, 2020).

Selain serangan *phishing*, serangan *ransomware* juga menjadi ancaman keamanan siber yang semakin meningkat. *Ransomware* adalah serangan di mana penyerang mengambil alih data korban dan meminta uang tebusan untuk memulihkan akses ke data tersebut. Menurut laporan Ransomware Attacks in 2020 dari Emsisoft, jumlah serangan *ransomware* meningkat sebesar 41% dari tahun sebelumnya. Serangan *ransomware* dapat menyebabkan kerusakan pada sistem informasi, kehilangan data, dan biaya yang besar untuk membayar tebusan (Emisoft, 2020).

Dalam beberapa tahun terakhir, wilayah ASEAN telah mengalami serangkaian serangan siber. Di Indonesia, angka serangan siber meningkat sebanyak 33% dari tahun 2014 ke 2015, dan Bank Indonesia mencatat peningkatan kejahatan siber sebesar 66,7% pada tahun 2015. Peretas-petas tersebut berhasil masuk ke dalam *Society for Worldwide Interbank Financial Telecommunication* atau SWIFT, jaringan komunikasi antar bank global yang menangani transaksi, dan berhasil meretas sistem beberapa bank di seluruh dunia, termasuk beberapa bank di wilayah ASEAN pada bulan Oktober 2016. Kementerian Pertahanan Singapura juga menjadi korban peretasan dalam sistem Internetnya pada awal tahun 2017, yang mengakibatkan kebocoran informasi pribadi sebanyak 850 tentara dan staf. Pada bulan Juni 2016, lebih dari 2.100 server yang dimiliki oleh bank, bisnis, dan lembaga pemerintah di Malaysia disusupi dan aksesnya dijual kepada peretas. Di Vietnam, terdapat serangan siber terhadap situs web dua bandara dan Vietnam Airlines pada bulan Juli 2016 (ACCS, 2017).

ASEAN tidak tinggal diam dalam menanggapi risiko ini, dan selama beberapa tahun terakhir, negara-negara anggota atau *ASEAN Member State* (AMS) telah bekerja sama dalam berbagai kesempatan untuk memperkuat keamanan siber di tingkat regional. Selama 11 tahun terakhir, AMS dan mitra dialog mereka telah aktif terlibat dalam ASEAN CERT Incident Drill (ACID) tahunan, yang bertujuan untuk menguji koordinasi antara tim-tim tanggap insiden dan prosedur penanganan insiden. Pada tahun 2012, *ASEAN Telecommunications Regulators Council* (ATRC), sebuah badan sektoral yang berada di bawah *Telecommunication and IT Minister Meetings* (TELMIN), membentuk *ASEAN Network Security Action*

*Council* (ANSAC) dengan tujuan mendorong kerja sama *CERT* dan berbagi pengetahuan dan keahlian di antara negara-negara anggota. Kerja sama antara *Telecommunication and IT Senior Officials Meetings* (TELSOM) dan mitra dialog seperti China dan Jepang juga telah berkontribusi dalam meningkatkan keamanan siber di tingkat regional. Selain itu, masing-masing AMS juga telah melakukan kolaborasi dengan mitra dialog mereka dalam upaya meningkatkan keamanan siber regional.

Pada Pernyataan Ketua ASEAN Summit di Vientiane 2016, para pemimpin ASEAN mengakui pentingnya keamanan siber dan menyambut baik penyelenggaraan Konferensi Tingkat Menteri ASEAN tentang Keamanan Siber (AMCC) yang pertama di Singapura pada Oktober 2016. Konferensi tersebut bertujuan untuk memfasilitasi kerja sama yang lebih besar dalam bidang keamanan siber di antara negara-negara anggota ASEAN dan melengkapi upaya-upaya yang sudah ada dalam memperkuat keamanan siber di wilayah ini (ASEAN Summit, 2016).

Dalam Pertemuan Menteri Telekomunikasi dan Teknologi Informasi ASEAN dan Pertemuan Terkait (TELMIN) ke-15, para Menteri ASEAN menekankan pentingnya upaya kolektif dalam memastikan ekosistem TIK yang aman di ASEAN. Mereka juga menyatakan visi untuk mendorong ekonomi digital yang aman, berkelanjutan, dan transformatif, serta mencapai Komunitas ASEAN yang inovatif, inklusif, dan terintegrasi (TELMIN, 2015).

Dalam Deklarasi Bersama Menteri Pertahanan ASEAN tentang Mempromosikan Kerja Sama Pertahanan untuk Komunitas ASEAN yang Dinamis

(ADMM), Pertemuan Menteri Pertahanan ASEAN mengekspresikan keprihatinan mereka terhadap ancaman non-tradisional yang semakin sering, besar, dan kompleks. Mereka menegaskan komitmen kolektif ADMM untuk mengatasi ancaman semacam itu guna mempromosikan perdamaian, keamanan, dan kemakmuran di wilayah ASEAN (ADMM, 2016).

Para menteri ASEAN tentang Kejahatan Transnasional (AMMTC) secara berkala menekankan pentingnya meningkatkan kerjasama dalam menghadapi tantangan kejahatan siber yang semakin kompleks di wilayah ASEAN. Mereka menyadari perlunya upaya bersama untuk mengatasi ancaman kejahatan siber yang semakin meningkat di kawasan ini dan menyadari pentingnya membangun kapasitas terkait keamanan siber bagi negara-negara ASEAN (AMTCC-Japan, 2015).

Untuk mencapai tujuan ini, ASEAN telah menyusun ASEAN Cybersecurity Cooperation Strategy I pada tahun 2017-2020. Tujuan strategi ini adalah menciptakan ruang siber yang aman dan terlindungi di wilayah ASEAN dengan meningkatkan kerjasama regional. Salah satu fokus strategi ini adalah memperkuat kerjasama antara Computer Emergency Response Team (CERT-CERT) dan meningkatkan kapasitas serta koordinasi inisiatif kerjasama keamanan siber di tingkat regional. Dengan demikian, strategi ini bertujuan untuk meningkatkan kemampuan regional dalam menghadapi ancaman siber yang semakin berkembang dan meningkatkan efisiensi sumber daya dengan menghindari duplikasi yang tidak efisien.

Dengan tujuan tersebut, *ASEAN TELMIN* menugaskan *ASEAN Network Security Action Council* (ANSAC) untuk menyiapkan makalah strategi ini guna memberikan peta jalan bagi kerja sama regional untuk mencapai tujuan ruang siber ASEAN yang aman dan terlindungi, yang juga akan membantu memperkuat keamanan informasi di ASEAN sejalan dengan dorongan strategis tentang Keamanan dan Jaminan Informasi dalam ASEAN *ICT Masterplan 2020* (AIM, 2020).

Strategi ini menyarankan bahwa sebagai langkah awal, TELMIN memberi mandat kepada TELSOM untuk mengidentifikasi, mengevaluasi, dan memperkuat kerja sama keamanan siber dalam tiga bidang utama, yaitu: (i) respons terhadap insiden keamanan siber, (ii) kebijakan dan koordinasi Tim Tanggap Darurat Komputer (*Computer Emergency Response Team/CERT*), dan (iii) pengembangan kapasitas keamanan siber.

Dalam mencapai tujuan Strategi dan untuk menjaga fokus pada area-area yang menjadi mandat TELMIN, strategi yang diajukan hanya akan berfokus pada peningkatan kerja sama keamanan siber di sektor sipil di dalam ruang siber. Bidang lain seperti kejahatan siber, pertahanan siber, dan diplomasi siber tidak akan menjadi bagian dari strategi ini karena saat ini tidak termasuk dalam mandat TELMIN.

ASEAN Ministerial Conference on Cybersecurity (AMCC) yang diselenggarakan di singapura pada 11 oktober 2016 membuat inisiasi dengan tujuan peningkatan kapasitas ASEAN dalam penanggulangan ancaman siber yang semakin marak terjadi di Kawasan Asia Tenggara. Dengan hal tersebut, negara-

negara dikawasan asia tenggara melihat adanya urgensi dalam menjalin kerjasama keamanan siber pada waktu dekat dengan tidak hanya membangun keamanan siber nasional namun bertingkat menjadi keamanan siber di tingkat regional yaitu Asia Tenggara (Parameswaran, 2016).

Negara-negara anggota ASEAN telah menyadari pentingnya menjaga keamanan siber dan infrastruktur teknologi informasi mereka, sehingga ASEAN Cyber Capacity Program dibentuk. Terdapat empat mekanisme ASEAN yang fokus pada aspek keamanan siber dan kejahatan siber, yaitu: ASEAN Ministerial Meeting on Transnational Crime (AMMTC), ASEAN Telecommunications and IT Ministers Meeting (TELMIN), ASEAN Regional Forum (ARF), dan ASEAN Senior Officials Meeting on Transnational Crime (SOMTC). AMMTC bertujuan meninjau isu-isu regional dan menetapkan agenda kerja sama antara lembaga pemerintah Asia Tenggara dalam mengatasi kejahatan transnasional termasuk cybercrime. SOMTC melaksanakan agenda AMMTC dan mengidentifikasi delapan wilayah kejahatan transnasional yang termasuk di dalamnya adalah cybercrime. Program-program ARF termasuk kegiatan seperti seminar, konferensi, dan lokakarya tentang siber terorisme, respon insiden siber, serta kesiapsiagaan dalam meningkatkan keamanan siber (Putra, 2018).

Pendanaan untuk sumber daya peningkatan keahlian dan pelatihan negara negara di ASEAN untuk membangun sarana dan prasarana untuk mitigasi, mencegah dan menanggulangi ancaman siber dilakukan oleh ASEAN Cyber Capacity Program (ACCP). Pada prosesnya diantara lain adalah pembangungan lokakarya, seminar dan konferensi, dan upaya untuk membuat undang-undang

strategis untuk melawan kejahatan siber dibawah perlindungan ASEAN. Pemegang kebijakan, aparatur teknis terkait, dan penegak hukum jaksa hingga analis serta diplomat dari seluruh negara di ASEAN dilibatkan menjadi target dalam upaya program ini. Pelatih program ini dipilih dari Pusat Global Inovasi INTERPOL di Singapura, Mitra Dialog ASEAN, akademisi dari Centre of Excellence for National Security (CENS) di Rajaratnam School of International Studies (RSIS), agen keamanan siber di Singapura dan agensi terkait lainnya. Kemudian akan dipublikasikan melalui rangkaian acara ASEAN dan perwakilan dari setiap negara ASEAN akan diundang untuk mendaftarkan diri kedalam cakupan ASEAN Cybersecurity Cooperation Strategy (ACCS) (CSA, 2016)..

Situasi keamanan siber di Indonesia selama beberapa tahun terakhir telah menghadapi berbagai tantangan yang signifikan. Sejak tahun 2017, negara ini telah menjadi target serangan siber yang beragam, termasuk serangan ransomware, serangan DDoS (Denial of Service), dan pencurian data. Salah satu contoh terkenal adalah serangan ransomware WannaCry yang melanda sejumlah lembaga penting di Indonesia seperti Rumah Sakit Harapan Kita, Rumah Sakit Dharmais, dan Universitas Jember. Serangkaian serangan ini menimbulkan kekhawatiran dan ketidakamanan di kalangan masyarakat. Meskipun ada upaya pemerintah untuk menghadapi serangan tersebut, namun tantangan keamanan siber yang semakin kompleks menuntut kerjasama yang lebih kuat dalam mengatasi ancaman ini.

ID-SIRTII/CC, sebagai Indonesia Security Incident Response Team on Internet Infrastructure Coordinator Center, telah melakukan pemantauan terhadap keamanan internet di Indonesia selama beberapa tahun. Menurut laporan mereka

pada tahun 2017, ada lebih dari 200 juta serangan yang terjadi selama 11 bulan. Aktivitas malware menjadi salah satu ancaman utama, dengan sekitar 36 juta aktivitas malware terdeteksi. Laporan tersebut juga mencatat variasi kondisi keamanan internet di Indonesia selama tahun itu, menunjukkan tingginya fluktuasi dan kompleksitas tantangan keamanan siber yang dihadapi.

Pemerintah Indonesia menyadari pentingnya mengatasi ancaman keamanan siber dan telah mengambil langkah-langkah strategis untuk memperkuat pertahanan siber negara. Pada tahun 2018, pemerintah meluncurkan Strategi Keamanan Siber Nasional yang bertujuan untuk meningkatkan keamanan siber melalui kerjasama antarinstansi, perusahaan, dan masyarakat. Peningkatan jumlah insiden keamanan siber di tahun 2019 menunjukkan perlunya lebih banyak investasi dan kesadaran tentang keamanan siber di Indonesia. Meskipun demikian, pemerintah dan lembaga terkait terus berupaya untuk meningkatkan kemampuan dan koordinasi guna menghadapi tantangan keamanan siber yang terus berkembang di tahun 2020 dan seterusnya.

Dengan masifmya rangkaian kejadian kejahatan siber diindonesia dalam kurun waktu 2017-2020 yang diakibatkan oleh kurangnya pemahaman negara maupun perusahaan membuat beberapa pihak menjadi resah kemudian menimbulkan sebuah gagasan atau ide dimana diperlukan suatu kerjasama untuk menjalin dan merangkai iklim perdagangan maupun stabilitas negara hingga Kawasan menjadi lebih terjamin dalam keamanan khususnya di ruang siber Kawasan Asia Tenggara  dengan segala infrastruktur yang berkaitan serta aspek

penting dalam suatu kepentingan agar terhindar dari pihak yang merugikan yaitu peretas.

Pemerintah Indonesia mendirikan Id-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure) dan BSSN (Badan Siber dan Sandi Negara) merupakan langkah penting dari pemerintah Indonesia dalam menghadapi tantangan keamanan siber yang semakin kompleks. Id-SIRTII berfungsi sebagai lembaga yang khusus mengawasi dan merespons insiden keamanan di infrastruktur dan jaringan Internet di Indonesia, sementara BSSN bertujuan menjadi lembaga pusat dalam pengelolaan keamanan siber nasional dan memastikan koordinasi efektif dalam menangani ancaman siber. Dengan adanya kedua lembaga ini, diharapkan Indonesia dapat lebih siap dan responsif dalam menghadapi serangan siber yang dapat merugikan negara dan masyarakat serta menciptakan lingkungan digital yang aman dan terlindungi bagi seluruh warganya. Kerjasama dan sinergi antara Id-SIRTII dan BSSN menjadi kunci untuk meningkatkan keamanan digital Indonesia secara efektif. Selain pada faktor kurangnya ketersediaan sumber daya manusia yang memiliki keahlian dalam bidang keamanan siber juga menjadi tantangan dalam meningkatkan kesiapan sistem keamanan siber Indonesia. Diperlukan upaya dalam meningkatkan keterampilan dan kualitas sumber daya manusia dalam bidang keamanan siber agar dapat mengidentifikasi, mencegah, dan menanggapi serangan siber dengan cepat dan efektif. Untuk mengatasi tantangan tersebut, perlu adanya kolaborasi antara pemerintah, bisnis, dan masyarakat untuk meningkatkan kesadaran dan keterampilan keamanan siber. Selain itu, pemerintah

juga harus meningkatkan investasi dalam sumber daya manusia, infrastruktur teknologi, dan sistem keamanan siber.

Dalam situasi yang semakin kompleks dan berubah-ubah, Pengaruh Kerjasama *ASEAN Cybersecurity Cooperation Strategy* terhadap Keamanan Siber Indonesia tahun 2017-2020 dengan acuan implementasi *ASEAN Cybersecurity Cooperation Strategy* I tahun 2017-2020 menjadi sangat penting untuk memastikan bahwa hasilnya dikemudian tentang kesiapan indonesia menghadapi ancaman keamanan siber di masa depan dengan integrasi dari organisasi internasional kawasan seperti ASEAN.

Berdasarkan penelitian terdahulu yang disusun oleh Maulia Jayanti Islami tahun 2017 dari Puslitbang Aptika dan IKP, Badan Litbang SDM, Kemenkominfo berjudul "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index". Peneliti telah menemukan persamaan dalam penelitian tersebut yang menganalisis dan melihat tantangan dalam pengimplementasian Strategi Keamanan Siber Nasional Indonesia dengan mengkaji beberapa unsur tantangan maupun kesiapan dalam upaya tersebut seperti persiapan dan potensi potensi ancaman lainnya yang akan dihadapi. Sedangkan yang menjadi pembeda nya adalah subjek dan objek peninjauan nya yang memiliki perbedaan. dimana dipenelitian tersebut meninjauh mengenai implementasi strategi dari Global Cybersecurity Index sedangkan ASEAN Cybersecurity Cooperation Strategy lebih memfokuskan pada integrasi Kawasan asia tenggara dalam menangani mencegah dan menganggulangi potensi ancaman siber yang ada.

Penelitian terkait juga disusun oleh Cynthia Rahmawati tahun 2019 dari Universitas Dirgantara Suryadarma mengenai “Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0”. Dimana peneiti menemukan persamaan pada objek penelitian yaitu keamanan siber di Indonesia melihat pada unsur tantangan dan ancaman yang berkorelasi langsung dengan analisis kesiapan sistem keamanan siber di indonesia. Dan hal yang menjadi pembeda maupun pelengkap nya yaitu pada penelitian peneliti menjadikan objek yang diteliti menjadi lebih luas serta lebih komprehensif sehingga menguatkan penelitian sebelum nya dimana hanya membahas tentang fenomena nasional nya saja sedangkan peneliti memperluas kajian hingga tingkat asia tengggara.

Pada tahun 2022,Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & Suwarno, P. Menyusun sebuah penelitian yang berjudul “Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. Jurnal Kewarganegaraan”, Dari Universitas Pertahanan Republik Indonesia, mengemukakan dan menjabarkan tentang bagaimana ancaman siber bisa dicari cara untuk memitigasi untuk mencari prioritas agar nantinya dijadikan untuk strategi dalam peningkatan keamanan siber Indonesia , dari bahasan tersebut terdapat kesamaan dalam objek penelitian yaitu sistem keamanan siber di Indonesia dimana penyusun mencari cara solusi dan upaya mitigasi hal serupa dalam pencegahan penanganan serangan siber di pada lingkup nasional. Sedangkan pada penelitian yang dibuat oleh peneliti memberi jangkauan yang lebih luas dalam referensi tentang cara menghadapi hal tersebut dengan menggunakan Kerjasama ASEAN Cybersecurity Cooperation Strategy yang dimana Kawasan asia tenggara berintegrasi untuk mencari solusi yang lebih

kompleks dan detail agar bisa terjadinya suatu timbal balik baik bantuan maupun dukungan dalam mencegah berbagai potensi ancaman siber yang terjadi di Indonesia maupun di asia tenggara.

Adi Rio Arianto dan Gesti Anggraini di tahun 2019 dari Universitas Pembangunan Nasional Veteran Indonesia membuat penelitian serupa dengan tajuk "Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team On Internet Infrastructure (Id-Sirtii)".Peneliti telah menemukan persamaan pada penelitian tersebut yaitu pembahasan tentang ancaman siber di Indonesia dengan mengkaji aspek pertahanan dan kesiapan dalam menghadapi serangan siber global dengan membentuk tim khusus didalam nya . Dan hal yang membedakan penelitian yaitu tentang cara implementasi yang mengharuskan pada tujuan dari ASEAN Cybersecurity Cooperation Strategy, sedangkan pada penelitian diatas mengenai tentang upaya inisiasi nasional dalam pembentuk ID-SIRTII dalam menanggapi ancaman siber. Terlebih lagi pada konteks yang memfokuskan penelitian pada masa pandemi dengan keterlibatan ASEAN sebagai kawasan yang mempunyai peran krusial dalam prosesnya tersebut.

Karya tulis ilmiah terakhir terkait yang disusun oleh Makbull Rizki di tahun 2022 dari Universitas Padjadjaran dengan isu yang dibahas yaitu "Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi".Peneliti telah menemukan persamaan pada penelitian tersebut yaitu pembahasan tentang Sistem keamanan siber di Indonesia dengan melihat perkembangan dan proses yang ada dalam tahap tersebut

yang dimana mengkaji bagaimana Indonesia dalam memfokuskan pada perkembangan sistem pertahanan dan keamanan siber nasional . Dan hal yang membedakan penelitian yaitu urgensi penelitian ini dibuat dengan mencari cara dalam menghadapi tantangan perkembangan teknologi informasi, sedangan penelitian peneliti membahas tentang ancaman serangan siber dan potensi nya yang ada di Kawasan Asia Tenggara melalui kerangka kerja ASEAN Cybersecurity Cooperation Strategy yang telah dirancang dan implementasi nya terhadap system keamanan siber di Indonesia itu sendiri.

Melihat pada beberapa komparasi penelitian dan permasalahan pada latar belakang, dengan tujuan untuk menjelaskan lebih dalam mengenai masalah inilah yang memotivasi peneliti untuk memberikan pembaruan dengan bangga mengajukan penelitian yang berjudul:

**"Pengaruh Kerjasama ASEAN Cybersecurity Cooperation Strategy terhadap Keamanan Siber Indonesia (2017-2020)".**

Maka dengan itu peneliti telah dibekali dengan pengetahuan dari beberapa mata kuliah yang terdapat pada Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Komputer Indonesia.antara lain sebagai berikut:

1. Regionalisme

   Mata kuliah ini mempelajari tentang keilmuan pada Kawasan Kawasan yang ada di seluruh dunia mulai dari Eropa, Asia, Afrika dsb. Dengan mempelajari *regionalism* peneliti mendapat pengetahuan mengenai keadaan di Kawasan, khususnya pada

penelitian ini yaitu keadaan Kawasan Asia Tenggara dengan melihat keadaan sosial politik dikawasan tersebut serta melihat bagaimana suatu melakukan interaksi dalam memenuhi kebutuhan maupun kepentingan satu sama lain.

2. Hubungan Internasional Asia Tenggara

   Mata kuliah ini mempelajari tentang fokus studi Kawasan Asia Tenggara yang dimana lebih mendalami berbagai unsur mulai dari hubungan antar negara di Asia Tenggara, mengenal komunitas regional seperti ASEAN, dan juga ekonomi sosial serta politik di asia tenggara yang dapat berguna pada penelitian ini agar bisa masuk kedalam pemahaman yang lebih mendalam kepada peran dan pengaruh Indonesia dalam menangani ancaman siber di asia tenggara.

3. Studi Keamanan Internasional

   Mata kuliah ini mempelajari tentang Keamanan Internasional yang dimana mempunyai fokus aspek keamanan di setiap bagian nya yang dipahami melalui berbagai materi tentang konflik/potensi konflik diberbagai belahan dunia dan bagaimana pandangan ilmu hubungan internasional dalam mengkaji nya, kaitan nya dengan penelitian ini yaitu keamanan siber merupakan materi turunan dari keamanan itu sendiri sehingga mempunya fokus yang sama tentang bagaimana

terjadinya konflik dan apa yang harus dilakukan untuk memahami nya.

4. Keamanan Siber

   Mata kuliah ini mempelajari tentang unsur spesifik dalam keamanan siber yaitu mulai dari apa yang dimaksud ruang siber, bagaimana kejahatan siber bias terjadi, serta potensi ancaman hingga cara menanggulangi nya dan memberi pengetahuan mengenai seluruh aspek yang dikaji dan melihat bagaimana keamanan siber diberbagai negara bekerja dalam hal ini sesuai judul penelitian, peneliti ingin mengkaji bagaimana kondisi keamanan siber di Indonesia dan bagaimana implikasi nya terhadap aspek kehidupan masyarakat untuk digunakan sebagai kajian untuk mencari solusi yang tepat atas permasalahan ancaman siber baik ditingkat nasional maupun regional pada tingkat Kawasan Asia Tenggara.

## 1.2 Rumusan Masalah

### 1.2.1. Rumusan Masalah Makro

Melihat dan didasari pada latar belakang masalah penelitian,untuk membantu menemukan pembahasan yang tepat dan sesuai tujuan maka peneliti telah menentukan rumusan masalah mayor sebagai berikut :

**“Bagaimana Pengaruh Kerjasama ASEAN *Cybersecurity Cooperation Strategy* berkontribusi terhadap Keamanan Siber Indonesia (2017-2020)?”**

### 1.2.2. Rumusan Masalah Mikro

Dari rumusan masalah mayor diatas, peneliti dielaborasikan kembali menjadi rumusan masalah minor yang ditujukan untuk pembahasan yang diharapkan menjadi lebih rinci. Maka peneliti merumuskan rumusan masalah minor antara lain:

1. Bagaimana kondisi Keamanan Siber di Indonesia sebelum *ASEAN Cybersecurity Cooperation Strategy I*?
2. Bagaimana *ASEAN Cybersecurity Cooperation Strategy I* tahun 2017-2020 diimplementasikan pada kebijakan dan strategi Keamanan Siber Indonesia selama 2017-2020?
3. Bagaimana kendala atau tantangan yang dihadapi dalam implementasi *ASEAN Cybersecurity Cooperation Strategy I* di Indonesia dalam periode 2017-2020?
4. Bagaimana Keamanan Siber Indonesia setelah adanya upaya implementasi yang dilakukan pemerintah Indonesia melalui *ASEAN Cybersecurity Cooperation Strategy* (2017-2020)?

### 1.2.3. Pembatasan Masalah

Adapun batasan masalah yang ditentukan peneliti yang hanya akan memberi fokus pada Pengaruh Kerjasama *ASEAN Cybersecurity Cooperation Strategy* terhadap Keamanan Siber Indonesia dengan rentang waktu analisis yang ditentukan yaitu dari tahun 2017 hingga 2020 dengan acuan hanya pada tahap pertama *ASEAN*

*Cybersecurity Cooperation Strateg*y yang disusun untuk tahun 2017 hingga 2020. Sehingga peneliti membatasi kurun waktu pada penelitian ini yaitu dari tahun 2017 hingga 2020 karena ingin menganalisis dan mengidentifikasi apakah Kerjasama tersebut berpengaruh secara efektif atau tidaknya setelah *ASEAN Cybersecurity Cooperation Strategy* I diimplementasikan. Dan hanya akan membahas tentang keamanan siber dengan batasan geografis yaitu di Asia Tenggara dimana ASEAN sendiri merupakan suatu komunitas regional diwilayah tersebut yang menjadikan fokus pembahasan yang nantinya akan dikaji peneliti melalui *ASEAN Cybersecurity Cooperation Strategy.*

## 1.3 Maksud dan Tujuan Penelitian

### 1.3.1 Maksud Penelitian

Bersumber pada latar belakang, rumusan masalah hingga pembatasan masalah yang dikaji peneliti agar dapat dijabarkan atas dasar maksud untuk mengetahui Bagaimana pengaruh dari kerjasama *ASEAN Cybersecurity Cooperation Strategy* terhadap Keamanan Siber Indonesia dalam kurun waktu 2017-2020.

### 1.3.2 Tujuan Penelitian

Dalam melengkapi penelitian, diperlukan untuk menentukan tujuan yang ingin dicapai oleh peneliti. Dengan adanya tujuan maka arah dari fokus menjadi lebih jelas, maka tujuan dari penelitian tentang Pengaruh Kerjasama ASEAN

Cybersecurity Cooperation Strategy terhadap Keamanan Siber Indonesia (2017-2020) sebagai berikut :

1. Untuk mengetahui tentang bagaimana kondisi Keamanan Siber di Indonesia sebelum dibuatnya ASEAN Cybersecurity Cooperation Strategy.
2. Untuk mengetahui dan menjelaskan ASEAN Cybersecurity Cooperation Strategy diimplementasikan pada kebijakan dan strategi Keamanan Siber Indonesia.
3. Untuk mengidentifikasi tentang bagaimana kendala atau tantangan yang dihadapi dalam implementasi ASEAN Cybersecurity Cooperation Strategy di Indonesia dalam periode 2017-2020.
4. Untuk menganalisis bagaimana Keamanan Siber Indonesia setelah adanya upaya implementasi yang dilakukan pemerintah Indonesia melalui ASEAN Cybersecurity Cooperation Strategy (2017-2020).

## 1.4 Kegunaan Penelitian

### 1.4.1 Kegunaan Teoritis

Hal yang diinginkan oleh peneliti dari penelitian ini adalah agar pembaca mendapat wawasan keilmuan serta tambahan informasi dan juga pengalaman dalam mengetahui suatu permasalahan yang ada. Sehingga pembaca pada penelitian ini akan mendapat pemahaman lanjutan terhadap Pengaruh Kerjasama ASEAN Cybersecurity Cooperation Strategy terhadap Keamanan Siber Indonesia (2017-2020).

### 1.4.2 Kegunaan Praktis

Dengan disusun nya penelitian ini,kegunaan praktis yang diharapkan oleh peneliti yaitu untuk memperoleh Gelar Sarjana S-1 (Strata Satu) pada Program Studi Ilmu Hubungan Internasional Universitas Komputer Indonesia. Serta kepada seluruh penstudi Ilmu Hubungan Internasional yang mempunyai minat dan ketertarikan pada keamanan siber maupun ASEAN juga dapat diharapkan terbantu oleh penelitian ini untuk menambah wawasan.