BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Pada studi Ilmu Hubungan Internasional terdapat dua istilah yang cukup melekat dan sering kali di sebut ke dalam pembahasannya, mereka adalah *high politics* dan *low politics. High politics* dapat diartikan sebagai hal utama yang diperlukan dari sebuah negara untuk menjaga kelangsungan hidup negara tersebut. Dan *low politics* sendiri diartikan sebagai isu-isu yang dianggap tidak terlalu penting atau tidak memiliki dampak yang signifikan terhadapan Keamanan nasional atau kepentingan negara yang vital. Dan masalah keamanan nasional terutama pada bidang militer masuk ke dalam kategori *high politics* Pada awalnya ancaman siber belum dianggap sebagai isu *high politics* oleh kebanyakan negara. Pada masa itu, ancaman siber dilihat sebagai ancaman siber biasa dan permasalahan keamanan informasi, bukan sebagai ancaman nasional yang signifikan.

Perkembangan teknologi dan infomasi yang sangat amat pesatlah yang mejadi salah satu faktor yang memberikan dampak yang besar dalam perkembangan teknologi informasi. Kemudian hadirnya internet sebagai bentuk teknologi yang makin memberikan dampak yang lebih, untuk mempermudah komunikasi dan informasi. Hadirnya internet juga yang menyebabkan banyak manusia yang tidak bisa terbebas dari aliran komunikasi dan infomasi. Internet telah menghasilkan kemajuan pesat di dalam kehidupan sehari-hari. Pada skala internasional, segala bentuk interaksi internasional telah dipengaruhi secara

signifikan oleh kemajuan teknologi. Mulai dari cara berkomunikasi dengan publik, melakukan negosiasi, menjalin kerjasama bilateral maupun multilateral dalam mencapai suatu kepentingan, jarang dilakukan dengan metode tradisional. Pendekatan modern yang berbasis teknologi dianggap lebih efisien dalam hal waktu, anggaran, dan aspek lainnya, sehingga metode tradisional mulai ditinggalkan dan digantikan dengan cara-cara yang memanfaatkan teknologi.

Selama sepuluh tahun terakhir, kemajuan di bidang teknologi informasi dan komunikasi (TIK) telah menyumbangkan dampak yang menguntungkan bagi pertumbuhan ekonomi dunia. Perkembangan TIK ini juga terkait erat dengan peningkatan produktivitas, daya saing usaha, serta partisipasi masyarakat dalam berbagai sektor (Setiadi, Sucahyo, & Hasibuan, 2012). Meski demikian, seiring meningkatnya konektivitas lembaga pemerintah, dunia usaha, dan masyarakat di dunia digital, muncul rintangan baru berupa ancaman siber yang membutuhkan fokus lebih untuk membangun sistem keamanan siber yang tangguh (Anjani, 2021). Oleh karena itu, penting untuk meningkatkan keamanan siber atau cybersecurity guna menghadapi bahaya dalam kejahatan teknologi informasi yang semakin berkembang. Keamanan siber merupakan sebuah aktivitas yang dilakukan untuk menjaga pengguna ruang siber dari berbagai bahaya yang ada di ruang siber (Satya & Agus , 2023). Dari hal di atas menjadikan keamanan siber menjadi esensial bagi sebuah negara karena mencakup berbagai faktor yang dapat berdampak pada keamanan keseluruhan negara.

Konsep *Internet of Things* (IoT) tersusun dari tiga elemen utama : pertama, objek fisik nyata yang telah diintegrasikan dengan modul sensor. Kedua, koneksi

internet yang memungkinkan objek-objek tersebut terhubung. Ketiga, pusat data di server yang berfungsi untuk mengamankan data atau informasi yang dikirimkan oleh aplikasi IoT. Penggunaan objek-objek yang terkoneksi internet ini akan menyatukan data yang akan diolah menjadi big data. Big data tersebut selanjutnya diproses dan dipelajari oleh berbagai pihak seperti lembaga pemerintah, perusahaan terkait, dan lembaga lainnya, untuk dimanfaatkan sesuai dengan kepentingan masing-masing (Triwahyuni, 2020).

Pada zaman digital yang kita jalani saat ini, ancaman terhadap keamanan siber menjadi semakin rumit dan bervariasi. Dalam kegiatan sehari-hari, kita memanfaatkan berbagai teknologi digital seperti smartphone, komputer, internet, serta perangkat Internet of Things atau IoT, yang menjadikan kita lebih rentan terhadap serangan siber dari kelompok yang tidak bertanggung jawab. *Malware* atau perangkat lunak berbahaya, dirancang untuk mengambil alih atau mengganggu infrastruktur komputer korbannya. Dengan menyamar sebagai file atau tautan yang tidak berbahaya, program-program ini mengelabui pengguna untuk mengunduhnya-sehingga memungkinkan akses asing tidak hanya ke komputer korban, tetapi juga ke seluruh jaringan di dalam sebuah organisasi. Motivasi utama dari serangan-serangan ini adalah untuk mencuri informasi pribadi atau perusahaan dan menyebabkan gangguan dalam operasi. Menurut laporan dari Statista pada tahun 2022, 5,5 miliar serangan *malware* terdeteksi di seluruh dunia dengan sebagian besar serangan ini terjadi di kawasan Asia Pacific (APAC). Di antara jenis serangan malware yang paling sering diblokir adalah *worm*, *virus*, *ransomware*, *trojan*, dan *backdoor* (Petrosyan, 2024).

Selain serangan *malware*, serangan *ransomware* juga menjadi ancaman bagi keamanan siber. *Ransomware* adalah jenis *malware* yang paling menguntungkan. Setelah mendapatkan akses ke perangkat dan file korban, pelaku ransomware mengenkripsi file-file tersebut dan meminta uang tebusan untuk mendekripsinya. *Ransomware* terutama disebarkan melalui lampiran email, iklan, URL, dan situs web. Pada tahun 2022, ada lebih dari 493 juta serangan *ransomware* di seluruh dunia (Petrosyan, 2024). Pada tahun 2023, lebih dari 72 persen bisnis di seluruh dunia terkena serangan *ransomware*. Angka ini menunjukkan peningkatan dari lima tahun sebelumnya dan sejauh ini merupakan angka tertinggi yang dilaporkan. Secara keseluruhan, sejak tahun 2018, lebih dari setengah dari total responden survei setiap tahun menyatakan bahwa organisasi mereka telah menjadi korban *ransomware* (Petrosyan, 2024). Industri manufaktur, bersama dengan sub industrinya, terus-menerus menjadi sasaran serangan *ransomware*, yang menyebabkan hilangnya data, gangguan bisnis, dan kerusakan reputasi. Seringkali, serangan siber semacam itu bersifat internasional dan memiliki tujuan politik. Industri manufaktur yang penting menduduki peringkat kedua dalam hal jumlah serangan ransomware, diikuti oleh industri fasilitas pemerintah.

Sejak pandemi Covid-19 melanda, isu serangan siber menjadi topik utama yang disoroti. Laporan dari Check Point Research (CPR) mengungkapkan bahwa wilayah Asia Pacific (APAC) mengalami lonjakan serangan siber sebesar 168% pada bulan Mei 2021 jika dibandingkan dari jangka waktu yang sama yaitu pada bulan Mei 2020. Negara-negara di kawasan Asia Pacific (APAC) yang mengalami peningkatan serangan siber terbesar adalah Jepang, Singapura, Indonesia, dan

Malaysia, dengan peningkatan masing-masing sebesar 40%, 30%, 25%, dan 22%. (Team, 2021). Sepanjang tahun 2021, serangan siber tidak hanya menjadi topik perbincangan yang ramai, tetapi juga menjadi insiden nyata yang menghiasi berita utama. Beberapa contohnya adalah sebagai berikut. Pada September di Malaysia, sebuah penyedia layanan hosting web diserang *ransomware* dengan permintaan tebusan *crypto* senilai US$900.000. Pada Mei, empat anak perusahaan dari sebuah perusahaan asuransi internasional di Thailand, Malaysia, Hong Kong, dan Filipina menjadi korban serangan *ransomware* dengan tuntutan tebusan US$20 juta. Pada September di Thailand, sistem komputer dan data milik sejumlah rumah sakit, perusahaan, dan organisasi dienkripsi serta diblokir akses. Insiden-insiden tersebut hanyalah sebagian kecil dari banyak kasus serangan siber yang terjadi (UNODC, 2021).

Dalam beberapa tahun terakhir wilayah Asia Pacific (APAC) telah mengalami insiden serangan siber. Di Indonesia juga mengalami insiden serangan siber, Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) menghitung sebanyak 88.414.296 serangan siber sejak 1 Januari hingga 12 April 2020. Pada Januari, terdeteksi 25.224.811 serangan, kemudian meningkat menjadi 29.188.645 serangan pada Februari. Jumlah serangan kembali menurun menjadi 26.423.989 kasus di bulan Maret, dan hingga 12 April 2020, tercatat 7.576.851 serangan. Puncak serangan terjadi pada 12 Maret 2020 dengan 3.344.470 kasus, namun jumlahnya mengalami penurunan secara signifikan setelah diterapkannya kebijakan *work from home* (WFH). Meski demikian, selama masa *work form home* (WFH), terjadi serangan siber dengan menggunakan isu

terkait yaitu Covid-19. Jenis serangan paling banyak adalah *trojan activity* sebesar 56%, diikuti *information gathering* (pengumpulan informasi) 43%, sedangkan sisanya 1% merupakan serangan *application attack* (BSSN, 2020). Kemudian pada mulai mei terjadi insiden besar yaitu bocornya 91 juta data dari platform Tokopedia dan diikuti insiden bocornya 5,8 juta data dari platform Red Doorz pada bulan November.

Pada tahun 2021 terjadinya peningkatan serangan siber yang sangat pesat terhadap keamanan siber Indonesia. Kelompok Operasi Deteksi, Penanggulangan dan Pemulihan, Penanganan Insiden dan Krisis Siber Nasional melakukan pemantauan anomali trafik terhadap Indonesia selama 7/24 jam dengan jumlah total anomali mencapai 1.637.973.002 miliar, Berdasarkah statistik monitoring, anomali tertinggi terjadi pada bulan Desember 2021 dengan jumlah anomali mencapai 242.066.168 anomali. Peningkatan ini terjadi mulai di bulan April, ada perbedaan klasifikasi anomali dari tahun sebelumnya, yang dimana tahun sebelumnya *trojan activity*. Pada tahun 2021 yang menyebabkan kenaikan angka serangan berasal dari *malware* (BSSN, 2021). Kenaikan angka serangan *malware* masih terjadi hingga bulan April tahun 2022. Kemudian di tahun 2022-2023 trafik anomali kembali stabil seperti di tahun 2020.

Situasi keamanan siber di Indonesia selama beberapa tahun terakhir telah menghadapi berbagai serangan yang signifikan. Negara ini telah menjadi target serangan siber yang beragam. Dalam langkah-langkah yang diambil untuk memperkuat upaya dalam meningkatkan keamanan siber, pemerintah menginisiasi Lembaga resmi negara yaitu Indonesia Security Incident Response Team on

Internet Infrastructure (Id-SIRTII/CC) didirikan pada tanggal 4 Mei 2007 mengacu pada Surat Keputusan Menteri Komunikasi dan Informasi nomor 26 tahun 2007. Id SIRTII/CC memiliki fungsi sebagai CERT/CSIRT Nasional dan Pusat Koordinasi Penanganan Insiden Nasional yang berada di bawah Direktorat Telekomunikasi Kementerian Komunikasi dan Informatika (KOMINFO). Selanjutnya pemerintah melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) dan peraturan perubahannya Peraturan Presiden Nomor 133 Tahun 2017 membentuk Badan Siber dan Sandi Negara (BSSN) yang bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber nasional. Setelah itu berdasarkan Peraturan Presiden nomor 53 tahun 2017, Id SIRTII/CC dilebur dan dipindahkan ke Badan Siber dan Sandi Negara dan bekerja di bawah Pusat Operasi Keamanan Siber Nasional BSSN sebagai Unit technostructure nya sejak April 2018 (Id-SIRTII, 2018).

Dengan keberadaan lembaga ini, diharapkan Indonesia dapat lebih siap dan tanggap menghadapi serangan siber yang dapat merugikan negara dan masyarakat, serta menciptakan lingkungan digital yang aman bagi seluruh warganya. Badan Siber dan Sandi Negara (BSSN) menjadi kunci penting untuk meningkatkan keamanan digital Indonesia secara efektif. Salah satu tantangan dalam meningkatkan kesiapan sistem keamanan siber Indonesia adalah minimnya ketersediaan sumber daya manusia yang memiliki keahlian di bidang keamanan siber. Pemerintah Indonesia menyadari urgensi dalam mengatasi ancaman keamanan siber dan telah mengambil langkah-langkah strategis untuk memperkuat

pertahanan siber nasional. Upaya peningkatan keterampilan dan kemampuan sumber daya manusia pada sektor ini sangat diperlukan agar dapat mengidentifikasi, mencegah, serta menanggapi serangan siber dengan cepat dan efektif. Kemudian upaya yang dilakukan adalah meluncurkan Strategi Keamanan Siber Nasional yang bertujuan untuk meningkatkan keamanan siber melalui kerjasama antara instansi pemerintah, perusahaan, dan masyarakat. Peningkatan jumlah insiden keamanan siber di tahun 2020-2023 menunjukkan perlunya peningkatan kesadaran tentang keamanan siber di Indonesia. Rangkaian kejadian kejahatan siber di Indonesia yang disebabkan oleh kurangnya pemahaman dari negara maupun perusahaan, dengan menuntut adanya kerjasama untuk menjalin dan menjaga stabilitas keamanan negara hingga kawasan Asia Pasifik agar lebih terjamin, khususnya dalam menjaga keamanan di ruang siber.

Computer Emergency Response Team (CERT) adalah sebuah organisasi yang bertanggung jawab untuk menangani insiden keamanan siber. Fungsi utama dari CERT yaitu bertugas menanggapi, menangani, dan mencegah insiden keamanan komputer dan jaringan, aktivitas yang di lakukan CERT berupa : peringatan dini tentang ancaman keamanan siber, menganalisis kerentanan sistem, merespon insiden keamanan siber yang terjadi dan melakukan koordinasi dengan pihak-pihak terkait untuk mengatasi masalah keamanan siber. Computer Security Incident Response Team (CSIRT) adalah dalah sebuah tim yang dibentuk untuk menangani insiden keamanan komputer dan jaringan dalam suatu organisasi atau entitas. Fungsi utama dan aktivitas yang dilakukan CSIRT ini hampir sama dengan CERT. Ada beberapa perbedaan diantara keduanya, cakupan CERT lebih luas dapat

beroperasi di tingkat nasional, organisasi, atau sektor tertentu, sedangkan cakupan CSIRT Cenderung lebih fokus pada organisasi tertentu, menangani insiden keamanan internal dalam lingkup perusahaan atau institusi spesifik. Kemudian dari segi tanggung jawab CERT memiliki mandat hukum atau pemerintah, terutama jika beroperasi di tingkat nasional, sedangkan CSIRT Tanggung jawab umumnya didefinisikan oleh kebijakan dan prosedur internal organisasi. Pembentukan CERT/CSIRT sangat penting untuk respons yang efektif dan efisien terhadap insiden keamanan komputer, kerentanan keamanan yang meluas dan koordinasi insiden di seluruh wilayah. Salah satu peran penting CERT/CSIRT adalah pendidikan dan pelatihan untuk meningkatkan meningkatkan kesadaran dan mendorong praktik terbaik. Perlunya kerjasama lintas CERTs/CSIRTs karena keterbukaan internet yang bersifat global membuat usaha pengamanan internet tidak dapat dilakukan sepihak. Motif insiden keamanan internet semakin kompleks dan dapat dilakukan lintas negara dalam waktu yang sangat singkat, sehingga mitigasi maupun penanganannya harus mampu menyesuaikan.

Dikawasan Asia Pacific (APAC) mempunyai organisasi kawasan di bidang keamanan siber yaitu Asia Pacific Emergency Response Team (APCERT) yang diadakan per tahun. Asia Pacific Computer Emergency Response Team (APCERT) adalah koalisi dari forum *Computer Emergency Response Teams* (CERTs) dan *Computer Security Incident Response Teams* (CSIRTs). Organisasi ini didirikan pada Februari 2003 untuk mendorong dan mendukung kegiatan CERTs/CSIRTs di wilayah Asia Pacific (APAC). Asia Pacific Computer Emergency Response Team (APCERT) di bentuk oleh 15 tim dari 12 Negara yang berbeda yaitu : Australia,

Vietnam, China, Hongkong, Indonesia, Jepang, Korea, Malaysia, Philippine, Singapura, Thailand dan China Taipei. Indonesia masuk ke dalam pembentukan organisasi Asia Pacific Computer Emergency Response Team (APCERT) melalui Indonesai Computer Emergency Response Team (ID-CERT). Pembentukan ID-CERT diawali dengan "nekat", berdasarkan pertimbangan belum adanya CERT di Indonesia pada saat itu, tahun 1998. Dengan bentuk informal dan yang lebih penting didaftarkan terlebih dulu, ID-CERT Indonesia Computer Emergency Response Team (ID-CERT) adalah CERT pertama di Indonesia yang berdiri secara independent, didirikan oleh DR. Budi Rahadjo tahun 1998. Tetapi ID-CERT hanya bersifat reaktif (tidak aktif) dalam merespon dan menangani kasus yang masuk atau dilaporkan oleh pelapor. Namun ID-CERT tidak memiliki berwenang untuk menangani keamanan siber Indonesia (ID-CERT, 2013).

Kemudian Indonesia melalui Indonesia Security Incident Response Team on Internet Infrastructure (Id-SIRTII) masuk ke dalam forum Asia Pacific Computer Emergency Response Team (APCERT) pada tanggal 4 Maret 2011 (APCERT, 2012). Dengan munculnya Id-SIRTII menjadikan lembaga pertama yang diberikan wewenang dalam menangani keamanan siber di Indonesia. Kemudian dibentuknya Badan Siber dan Sandi Negara (BSSN) pada tahun 2017, setelah itu pada tanggal 28 April 2018 Indonesia Security Incident Response Team on Internet Infrastructure (Id-SIRTII/CC) bergabung dengan Badan Siber dan Sandi Negara (BSSN). Id SIRTII/CC dilebur dan dipindahkan ke Badan Siber dan Sandi Negara dan bekerja di bawah Pusat Operasi Keamanan Siber Nasional BSSN sebagai Unit technostructure nya (Id-SIRTII, 2018). Keterlibatan Indonesia dalam

kerjasama dan koordinasi lintas negara pada organisasi Asia Pacific Computer Emergency Response Team (APCERT) merupakan refleksi upaya Pemerintah untuk memperkuat keamanan siber di Indonesia (SDPPI KOMINFO, 2012).

Asia Pacific Computer Emergency Response Team (APCERT), yang dibentuk pada tahun 2003 sebagai wadah bagi Computer Emergency Response Teams (CERTs) dan Computer Security Incident Response Teams (CSIRTs) di kawasan Asia Pasifik, yang di adakan secara rutin setiap tahunnya. Asia Pacific Computer Emergency Response Team (APCERT) memiliki misi untuk memelihara jaringan kontak yang terpercaya dari para ahli keamanan komputer di kawasan Asia Pacific (APAC) serta untuk meningkatkan kesadaran dan kompetensi Kawasan terkait dengan insiden keamanan komputer. Pertemuan ini bertujuan untuk mempertemukan para CERTs/CSIRTs dalam merumuskan strategi untuk penanganan insiden keamanan di kawasan ini. Dan strategi tersebut akan dibawa untuk di implementasikan pada keamanan siber dari masing-masing negara anggota. Selain itu, pertemuan ini juga berfungsi untuk membangun dan memperkuat rasa saling percaya antar CERTs/CSIRTs yang tergabung dalam organisasi tersebut.

Asia Pacific Computer Emergency Response Team (APCERT) memiliki beberapa agenda tahunan yang bertujuan untuk meningkatkan kerjasama antar anggotanya dan memperkuat keamanan siber di kawasan Asia Pasifik. Berikut adalah beberapa agenda tahunan yang diselenggarakan oleh APCERT (APCERT, Events APCERT) :

1. Annual General Meeting (AGM), diadakan setiap tahun yang memiliki tujuan untuk membahas laporan tahunan, mengevaluasi kinerja,

memperkuat kerjasama, dan merumuskan rencana strategis guna menjaga keamanan siber di wilayah Asia Pasifik..

2. APCERT Drill, diadakan sekali pada setiap tahunnya yang memiliki tujuan pelatihan siber skala besar yang melibatkan tim CERT dari berbagai negara untuk menguji kemampuan dalam merespon serangan siber. Latihan ini mencakup skenario serangan siber yang kompleks dengan fokus pada kerjasama lintas negara. Dan tema yang diangkat dalam APCERT Drill ini berbeda pada setiap tahunnya, tema tersebut ditentukan dari maraknya insiden dan isu-isu yang sering terjadi pada tahun itu.
3. Working Group (WGs), diadakan secara berkala sepanjang tahun yang memiliki tujuan untuk menangani topik atau bidang khusus yang penting bagi keamanan siber di kawasan Asia Pasifik. Setiap Working Group terdiri dari anggota APCERT yang memiliki keahlian atau minat dalam topik tertentu. Mereka bekerja sama untuk mencapai tujuan spesifik, seperti pengembangan teknologi, analisis ancaman, peningkatan kapasitas, atau pembentukan standar keamanan siber. APCERT memiliki banyak Working Group, berikut adalah WGs yang diikuti Indonesia diantaranya :
    - TSUBAME Working Group (di bentuk tahun 2009) adalah kelompok kerja yang bertujuan untuk memantau dan menganalisis lalu lintas jaringan guna mendeteksi dan memahami tren serangan siber di wilayah Asia Pasifik. TSUBAME sendiri adalah sistem pemantauan berbasis sensor yang dioperasikan oleh berbagai tim tanggap darurat (CERTs/CSIRTs) di bawah koordinasi APCERT.

- Information Sharing Working Group (di bentuk tahun 2011) adalah kelompok kerja yang bertujuan untuk memfasilitasi dan mengoordinasikan pertukaran informasi yang cepat dan efektif antar anggota APCERT, terutama terkait dengan insiden keamanan siber, tren ancaman, dan kerentanan. Fokus utama dari kelompok kerja ini adalah memastikan bahwa tim tanggap darurat keamanan komputer (CERT/CSIRT) di kawasan Asia Pasifik dapat saling berbagi informasi yang relevan secara real-time, sehingga memperkuat kemampuan kolektif dalam merespons ancaman siber.
- Internet of Thingking Security Working Group (di bentuk tahun 2017) adalah kelompok kerja yang berfokus pada isu-isu keamanan terkait IoT di kawasan Asia Pasifik. Kelompok ini bertujuan untuk mengidentifikasi, menganalisis, dan mengatasi ancaman keamanan yang muncul dari perangkat IoT yang semakin meluas penggunaannya.
- Membership Working Group (di bentuk tahun 2011) adalah kelompok kerja yang bertanggung jawab untuk mengelola dan mengawasi segala hal terkait keanggotaan organisasi. MWG memiliki peran penting dalam menjaga kualitas dan integritas anggota APCERT, serta memastikan bahwa organisasi terus berkembang dengan anggota yang memenuhi syarat dan berkomitmen terhadap tujuan APCERT.

- Trainning Working Group (di bentuk tahun 2015) adalah kelompok kerja yang bertugas mengembangkan, mengoordinasikan, dan memberikan pelatihan yang berkaitan dengan keamanan siber bagi anggota APCERT. Kelompok ini bertujuan untuk meningkatkan keterampilan teknis, pengetahuan, dan kapasitas tim CERT/CSIRT di kawasan Asia Pasifik, sehingga mereka dapat merespons ancaman siber dengan lebih efektif dan cepat (APCERT, Working Groups).

Sejalan dengan arus perkembangan teknologi yang terus berlanjut, konsep keamanan dalam konteks sebuah negara pun mengalami transformasi yang signifikan. Perhatian tidak lagi hanya terfokus pada aspek fisik atau teritorial semata, melainkan juga pada dimensi keamanan dalam dunia maya atau siber. Pengaruh Kerjasama Asia Pacific Computer Emergency Response Team (APCERT) terhadap keamanan siber Indonesia menjadi begitu penting untuk memastikan kesiapan Indonesia menghadapi ancaman siber di masa yang akan datang dengan integrasi dari organisasi Kawasan Asia Pacific (APAC).

Berdasarkan penelitian terdahulu yang disusun oleh Yusep Ginanjar tahun 2022 dari Universitas Jendral Acmad Yani yang berjudul “Strategi Indonesia Membentuk *Cyber Security* Dalam Menghadapi Ancaman *Cyber Crime* Melalui Badan Siber dan Sandi Negara”. Peneliti telah menemukan persamaan dalam penelitiannya yang menganalisis tantangan Badan Siber dan Sandi Negara dalam membentuk *cyber security* di Indonesia serta strategi Badan Siber dan Sandi Negara dalam membentuk *cyber security* di Indonesia. Sedangkan yang menjadi pembeda

dari penelitian ini adalah objek penelitiannya. Dimana penelitian ini menganalisis Kerjasama Indonesia dengan Asia Pacific Computer Emergency Response Team (APCERT), yang akan di implementasikan pada keamanan siber Indonesia.

Penelitian lainnya yang terkait juga disusun oleh Yudha Wahyu Nugraha tahun 2023 dari Universitas Komputer Indonesia yang berjudul "Pengaruh Kerjasama *ASEAN CYBERSECURITY COOPERATION STRATEGY* terhadap Keamanan Siber Indonesia. Peneliti telah menemukan persamaan objek dalam penelitiannya yang menganalisis perngaruh kerjasama terhadap keamanan siber Indonesia. Sedangkan yang menjadi pembeda dari penelitiannya adalah subjek penelitiannya. Dimana penelitian ini menganalisis Kerjasama Indonesia dengan Asia Pacific Computer Emergency Response Team (APCERT), yang akan di implementasikan pada keamanan siber Indonesia.

Penelitian lainnya yang terkait juga disusun oleh Cynthia Rahmawati tahun 2019 dari Universitas Dirgantara Suryadama yang berjudul "Tantangan dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0". Peneliti telah menemukan persamaan dalam penelitiannya yang menganalisis keamanan siber di Indonesia pada unsur tantangan dan ancamannya. Sedangkan yang menjadi pembeda dari penelitiannya adalah subjek penelitiannya. Dimana penelitian ini menganalisis Kerjasama Indonesia dengan Asia Pacific Computer Emergency Response Team (APCERT), yang akan di implementasikan pada keamanan siber Indonesia, dan penelitian sebelumnya hanya membahas tentang fenomena nasional nya saja sedangkan peneliti memperluas kajian hingga tingkat Asia Pacific (APAC).

Penelitian lainnya yang terkait juga disusun oleh Satya Muhammad Sutra dan Agus Haryanto tahun 2023 dari Universitas Jendral Soedirman yang berjudul "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020". Peneliti telah menemukan persamaan dalam penelitiannya yang menganalisis keamanan siber di Indonesia. Sedangkan yang menjadi pembeda dari penelitiannya adalah objek penelitiannya. Dimana penelitian ini menganalisis Kerjasama Indonesia dengan Asia Pacific Computer Emergency Response Team (APCERT), yang akan di implementasikan pada keamanan siber Indonesia.

Penelitian terdahulu terakhir terkait yang disusun oleh Makbull Rizki tahun 2022 dari Universitas Padjadjaran yang berjudul "Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi". Peneliti telah menemukan persamaan dalam penelitiannya yang berisi tentang sistem keamanan siber di Indonesia dengan melihat perkembangannya. Sedangkan yang menjadi pembeda dari penelitiannya adalah subjek dan objek penelitiannya. Dimana penelitian ini menganalisis Kerjasama Indonesia dengan Asia Pacific Computer Emergency Response Team (APCERT), yang akan di implementasikan pada keamanan siber Indonesia.

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

“Pengaruh Asia Pacific Computer Emergency Response Team (APCERT) Terhadap Keamanan Siber Indonesia”

Maka dengan ini peneliti telah dibekali dengan pengetahuan dari beberapa mata kuliah yang ada 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 ilmu pengetahuan tentang berbagai kawasan di seluruh dunia, mulai dari Eropa, Asia, Afrika, dan lainnya. Dengan mempelajari regionalisme, peneliti mendapatkan pemahaman tentang kondisi di kawasan tertentu, khususnya dalam penelitian ini adalah keadaan di Kawasan Asia Tenggara. Hal ini dilakukan dengan mengamati situasi sosial politik di kawasan tersebut serta cara suatu wilayah berinteraksi untuk memenuhi kebutuhan dan kepentingan satu sama lain.

2. Hubungan Internasional di Asia Tenggara

   Mata kuliah ini berfokus pada studi Kawasan Asia Tenggara dengan mempelajari berbagai unsur secara mendalam, seperti hubungan antar negara di Asia Tenggara, memahami komunitas regional seperti ASEAN, serta mengkaji kondisi ekonomi, sosial, dan politik di kawasan tersebut. Pendalaman materi ini berguna untuk penelitian agar dapat memperoleh pemahaman yang lebih mendalam mengenai peran dan pengaruh Indonesia dalam menangani ancaman siber di wilayah Asia Tenggara.

3. Studi Keamanan Internasional

Mata kuliah ini mempelajari tentang Keamanan Internasional yang memiliki fokus pada aspek-aspek keamanan di berbagai wilayah dengan memahami berbagai materi mengenai konflik/potensi konflik di berbagai belahan dunia dan bagaimana sudut pandang ilmu hubungan internasional dalam mengkajinya. Kaitannya dengan penelitian ini adalah keamanan siber merupakan bagian turunan dari keamanan itu sendiri, sehingga memiliki fokus yang sama tentang bagaimana konflik dapat terjadi dan apa yang harus dilakukan untuk memahaminya.

4. Keamanan Siber

   Mata kuliah ini mempelajari unsur-unsur spesifik dalam keamanan siber, mulai dari pengertian ruang siber, bagaimana kejahatan siber dapat terjadi, potensi ancaman yang ada, serta cara untuk menanggulanginya. Mata kuliah ini memberikan pengetahuan mengenai seluruh aspek yang dikaji dan melihat bagaimana keamanan siber di berbagai negara bekerja. Dalam konteks penelitian ini, peneliti ingin mengkaji kondisi keamanan siber di Indonesia dan implikasinya terhadap berbagai aspek kehidupan masyarakat. Kajian ini digunakan untuk mencari solusi yang tepat atas permasalahan ancaman siber baik di tingkat nasional maupun regional, khususnya di Kawasan Asia Tenggara.

1.2 Rumusan Masalah

1.2.1 Rumusan Masalah Mayor

Berdasarkan latar belakang diatas dan untuk memudahkan peneliti membuat pembahasan yang tepat dan sesuai tujuan maka peneliti telah menentukan rumusan masalah mayor sebagai berikut :

“Bagaimana Pengaruh Asia Pacific Computer Emergency Response Team (APCERT) Terhadap Keamanan Siber Indonesia?”

1.2.2 Rumusan Masalah Minor

Dari rumusan masalah mayor, kemudian dapat diturunkan menjadi rumusan masalah minor yang ditujukan untuk pembahasan yang diharapkan menjadi lebih rinci. Maka peneliti merumuskan rumusan masalah minor antara lain :

1. Bagaimana upaya yang di lakukan Indonesia melalui Asia Pacific Computer Emergency Response Team (APCERT) untuk di implementasikan pada keamanan siber Indonesia?
2. Bagaimana kendala atau tantangan yang dihadapi Indonesia melalui Asia Pacific Computer Emergency Response Team (APCERT) dalam implementasi pada keamanan siber Indonesia?
3. Bagaimana keamanan siber Indonesia setelah adanya upaya yang dilakukan Indonesia melalui Asia Pacific Computer Emergency Response Team (APCERT)?

1.2.3 Pembatasan Masalah

Adapun batasan masalah yang ditentukan peneliti hanya akan memberikan fokus pada Pengaruh Asia Pacific Computer Emergency Response Team (APCERT) Terhadap Keamanan Siber Indonesia dengan rentang waktu analisis yang ditentukan yaitu dari tahun 2020 hingga 2023. Peneliti memilih kurun waktu tersebut di dasari dari adanya kenaikan insiden serangan siber yang terjadi di Indonesia pada tahun tersebut.

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 Pengaruh Asia Pacific Computer Emergency Response Team (APCERT) Terhadap Keamanan Siber Indonesia.

1.3.2 Tujuan Penelitian

Untuk melengkapi penelitian, diperlukan tujuan yang ingin dicapai oleh peneliti. Dengan adanya tujuan menjadi lebih fokus dan sesuai, maka tujuan dari penelitian ini mengetahui Asia Pacific Computer Emergency Response Team (APCERT) Terhadap Keamanan Siber Indonesia sebagai berikut :

1. Untuk mengetahui upaya yang di lakukan Indonesia melalui Asia Pacific Computer Emergency Response Team (APCERT) untuk di implementasikan pada keamanan siber Indonesia.

2. Untuk mengetahui kendala atau tantangan yang dihadapi Indonesia melalui Asia Pacific Computer Emergency Response Team (APCERT) dalam implementasi pada keamanan siber Indonesia.
3. Untuk mengetahui keamanan siber Indonesia setelah adanya upaya yang dilakukan Indonesia melalui Asia Pacific Computer Emergency Response Team (APCERT).

1.4 Kegunaan Penelitian

1.4.1 Kegunaan Teoritis

Penelitian ini bertujuan untuk memberikan wawasan keilmuan, informasi tambahan, serta pengalaman kepada pembaca dalam memahami suatu permasalahan yang ada. Dengan demikian, pembaca akan mendapatkan pemahaman lebih lanjut mengenai Asia Pacific Computer Emergency Response Team (APCERT) Terhadap Keamanan Siber Indonesia.

1.4.2 Kegunaan Praktis

Dengan penyusunan penelitian ini, kegunaan praktis yang diharapkan oleh peneliti adalah untuk memperoleh gelar Sarjana S-1 (Strata Satu) pada Program Studi Ilmu Hubungan Internasional di Universitas Komputer Indonesia. Selain itu, penelitian ini juga diharapkan dapat membantu dan menambah wawasan bagi seluruh penstudi Ilmu Hubungan Internasional yang memiliki minat dan ketertarikan dalam bidang keamanan siber maupun Asia Pacific (APAC).