# BAB 1

# PENDAHULUAN

## A. Latar Belakang

Di tengah pesatnya perkembangan teknologi digital, kawasan Asia Tenggara menjadi salah satu wilayah dengan tingkat penetrasi internet yang tinggi. Hal ini turut mempengaruhi bagaimana masyarakat dan pemerintah di negara-negara ASEAN menggunakan teknologi informasi dalam berbagai aspek kehidupan, seperti pemerintahan, ekonomi, dan sosial. Namun, seiring dengan perkembangan ini, ancaman terhadap keamanan digital atau kejahatan siber juga meningkat. Kejahatan siber lintas negara semakin menjadi ancaman serius, mengingat bahwa sebagian besar negara anggota ASEAN memiliki keterkaitan ekonomi dan jaringan digital yang erat.

Di era digital saat ini, kejahatan siber menjadi ancaman serius bagi stabilitas nasional dan regional, terutama bagi negara-negara di ASEAN. Dengan meningkatnya ketergantungan pada teknologi informasi dan komunikasi, keamanan siber menjadi fokus penting untuk melindungi informasi sensitif, menjaga integritas sistem, dan melindungi privasi pengguna. ASEAN, sebagai organisasi regional, melihat perlunya kerja sama dalam menghadapi tantangan ini, terutama dengan meningkatnya ancaman siber lintas batas negara.Menurut laporan dari Interpol, kejahatan siber di Asia Tenggara terus meningkat dalam beberapa tahun terakhir, dengan serangan yang semakin kompleks dan merugikan. Oleh karena itu, kerja sama antar negara dalam mengatasi kejahatan siber menjadi sangat penting.

Kejahatan siber di ASEAN telah menjadi isu krusial seiring dengan meningkatnya ketergantungan pada teknologi dan internet di kawasan ini. Kejahatan siber mencakup berbagai tindakan ilegal yang dilakukan melalui jaringan komputer, termasuk pencurian data pribadi, serangan ransomware, dan penipuan online. Menurut laporan dari United Nations Office on Drugs and Crime (2021), kejahatan siber telah memberikan dampak signifikan pada stabilitas ekonomi dan keamanan di Asia Tenggara, dengan jutaan dolar hilang akibat serangan ini setiap tahunnya. ASEAN telah mengidentifikasi keamanan siber sebagai prioritas utama, sebagaimana tertuang dalam "ASEAN Cybersecurity Cooperation Strategy" (ASEAN, 2020), yang bertujuan untuk meningkatkan kerja sama regional dalam menangani ancaman ini. Interpol (2022) juga melaporkan bahwa operasi kejahatan siber di kawasan ini seringkali melibatkan pelaku lintas negara, menjadikan koordinasi antar negara anggota ASEAN sangat penting. Berdasarkan berbagai fakta tersebut, dapat disimpulkan bahwa kejahatan siber di ASEAN merupakan ancaman yang kompleks dan memerlukan upaya kolektif dari semua negara anggota untuk menanggulanginya secara efektif.

Pada konteks ini, Malaysia memegang peranan vital dalam upaya kolaboratif menangani isu kejahatan siber di ASEAN. Sebagai salah satu pionir dalam pengembangan kebijakan siber di kawasan, Malaysia telah berpartisipasi aktif dalam forum kerja sama keamanan siber ASEAN. Cybersecurity Malaysia (2021) menyatakan bahwa negara ini telah mengimplementasikan sejumlah program dan inisiatif yang bertujuan untuk

meningkatkan kemampuan deteksi dan penanggulangan ancaman siber. Lebih lanjut, laporan tahunan ini menunjukkan bahwa sinergi antara sektor publik dan swasta di Malaysia berperan dalam penguatan pertahanan siber nasional yang dapat dijadikan model bagi negara-negara ASEAN lainnya. Keberhasilan ini menandakan bahwa dengan strategi yang tepat dan kerja sama yang solid, tantangan yang dihadapi oleh negara-negara ASEAN dalam menangani kejahatan siber dapat diatasi. Kesimpulannya, peran aktif Malaysia dalam forum kerja sama keamanan siber ASEAN merupakan contoh penting dari bagaimana upaya terkoordinasi dapat membawa keberhasilan dalam mengatasi ancaman kejahatan siber di kawasan.

ASEAN Cybersecurity Cooperation Forum dibentuk sebagai platform untuk kolaborasi antara negara-negara anggota ASEAN dalam memperkuat keamanan siber di kawasan. Forum ini bertujuan untuk meningkatkan kesadaran, berbagi informasi, serta menyusun kebijakan yang dapat menanggulangi kejahatan siber.

Peran Malaysia sangat menonjol dalam forum ini, karena negara tersebut memiliki kebijakan keamanan siber yang kuat dan pengalaman dalam menangani insiden siber. Malaysia berperan sebagai fasilitator dan penggerak dalam berbagai inisiatif keamanan siber di ASEAN.

Dokumen "ASEAN Cybersecurity Cooperation Strategy" (ASEAN, 2020) menyoroti pentingnya kolaborasi antar negara anggota untuk mengatasi ancaman siber yang semakin kompleks. Dokumen ini menyebutkan bahwa sinergi antara sektor publik dan swasta sangat penting

untuk memastikan keamanan siber yang efektif di kawasan ASEAN. Selain itu, strategi ini juga menekankan perlunya pendekatan multilayered untuk menangani kejahatan siber, dan Malaysia berkontribusi dalam implementasi strategi ini melalui berbagai inisiatif.

Interpol dalam laporan "ASEAN Sibercrime Operations" (2022) menggambarkan operasi yang difasilitasi di kawasan ini yang menunjukkan peningkatan deteksi dan penuntutan kejahatan siber. Operasi ini melibatkan kolaborasi lintas negara, di mana Malaysia memainkan peran sentral dalam menyediakan keahlian teknis dan dukungan operasional untuk mengatasi ancaman siber. Dalam konteks ini, Malaysia diakui sebagai salah satu negara penggerak utama yang mendukung operasionalisasi strategi keamanan siber ASEAN.

Laporan dari United Nations Office on Drugs and Crime (UNODC, 2021) mengenai "Sibercrime and Its Impact in Southeast Asia" juga menggarisbawahi bagaimana kejahatan siber berdampak pada kawasan ini, dengan penekanan pada perlunya respons kolektif. Malaysia sekali lagi muncul sebagai pemimpin regional, memanfaatkan pengalamannya dalam pengelolaan keamanan siber untuk membangun kapasitas negara-negara tetangga.

Penguatan strategi keamanan siber di ASEAN tidak terlepas dari dinamika hubungan antara negara-negara anggotanya. Scholarly articles yang mempelajari peran negara-negara anggota, khususnya Malaysia, menyebutkan pentingnya diplomasi siber dalam memperkuat kerja sama.

Negosiasi dan dialog terus dilakukan untuk memastikan bahwa semua negara anggota memiliki kapasitas yang memadai dalam mengatasi ancaman siber.

Kondisi faktual ini juga menunjukkan adanya kebutuhan mendesak untuk membangun kerangka kerja sama yang lebih komprehensif. Malaysia, dengan pengalamannya di bidang keamanan siber, diharapkan dapat terus memberikan kontribusi positif dalam forum kerja sama ini. Melalui berbagi pengetahuan dan teknologi, negara ini dapat membantu negara-negara anggota lain dalam mengembangkan kapabilitas mereka dalam menghadapi ancaman siber.

Kejahatan siber di ASEAN telah menunjukkan peningkatan yang signifikan dalam beberapa tahun terakhir. Menurut laporan dari ASEAN Cybersecurity Cooperation Strategy, kejahatan siber seperti penipuan online, pencurian data, dan serangan ransomware semakin marak terjadi di kawasan ini (ASEAN, 2020). Dalam konteks ini, ASEAN mencatat bahwa lebih dari 60% perusahaan di kawasan ini pernah mengalami insiden keamanan siber dalam lima tahun terakhir, dengan dampak finansial yang besar bagi mereka.

Salah satu contoh nyata dari ancaman kejahatan siber di ASEAN adalah serangan ransomware yang menargetkan sektor kesehatan selama pandemi COVID-19. Di Malaysia, misalnya, beberapa rumah sakit dan fasilitas kesehatan mengalami serangan yang mengakibatkan gangguan layanan dan pencurian data pasien. Menurut laporan dari Kementerian Kesihatan Malaysia, lebih dari 30% rumah sakit di Malaysia melaporkan insiden keamanan siber selama tahun 2021 (Kementerian Kesihatan

Malaysia, 2021). Hal ini menunjukkan betapa rentannya sektor kesehatan terhadap serangan siber, dan pentingnya perlindungan yang lebih baik.

Di negara-negara lain di ASEAN, seperti Indonesia dan Filipina, kejahatan siber juga menunjukkan tren yang mengkhawatirkan. Indonesia, sebagai salah satu negara dengan pengguna internet terbesar di ASEAN, mencatat lebih dari 1 juta insiden kejahatan siber pada tahun 2020 saja. Menurut Badan Siber dan Sandi Negara (BSSN), angka ini meningkat hampir 30% dibandingkan tahun sebelumnya (BSSN, 2020). Sementara itu, Filipina mengalami lonjakan serangan phishing yang menargetkan pengguna internet, terutama selama periode lockdown akibat pandemi.

Keberadaan infrastruktur digital yang semakin berkembang di ASEAN juga menjadi faktor pendorong meningkatnya kejahatan siber. Dengan semakin banyaknya transaksi online dan pertumbuhan e-commerce, pelaku kejahatan siber semakin berani untuk melakukan aksinya. Data dari Statista menunjukkan bahwa nilai pasar e-commerce di ASEAN diperkirakan mencapai USD 102 miliar pada tahun 2025, yang tentunya menarik perhatian pelaku kejahatan siber (Statista, 2021).

Dalam menghadapi tantangan ini, kolaborasi antarnegara di ASEAN menjadi sangat penting. Melalui ACCF, negara-negara anggota dapat saling berbagi informasi mengenai ancaman siber, teknik mitigasi, dan praktik terbaik dalam penanganan insiden. Selain itu, pelatihan dan pengembangan kapasitas di bidang keamanan siber juga perlu ditingkatkan untuk memastikan bahwa seluruh negara anggota siap menghadapi ancaman yang

ada. Dengan demikian, upaya bersama dalam menangani kejahatan siber di ASEAN dapat memberikan perlindungan yang lebih baik bagi masyarakat dan ekonomi di kawasan ini.

Peran Malaysia dalam ASEAN Cybersecurity Cooperation Forum merupakan elemen kunci dalam upaya penanggulangan kejahatan siber di kawasan Asia Tenggara. Secara khusus, Malaysia telah menunjukkan komitmen yang kuat dalam memperkuat keamanan siber regional melalui inisiatif dan kebijakan yang diterapkan di dalam forum ini. Berdasarkan dokumen "ASEAN Cybersecurity Cooperation Strategy" (2020), salah satu fokus utama dari strategi keamanan siber ASEAN adalah memperkuat kolaborasi intra-regional guna memastikan keseimbangan keamanan digital di antara negara-negara anggotanya. Malaysia, dengan sumber daya dan keahlian yang dimilikinya, telah berperan penting dalam meningkatkan kemampuan dan kapasitas keamanan siber ASEAN. Sejalan dengan itu, laporan tahunan dari Cybersecurity Malaysia (2021) menyoroti sejumlah program dan kebijakan nasional yang mendukung tujuan forum dalam memitigasi ancaman siber yang semakin kompleks. Program-program ini menjadi model bagi negara anggota lainnya dalam mengembangkan rencana aksi siber nasional yang efektif.

Malaysia memainkan peran yang sangat penting dalam ACCF, tidak hanya untuk kepentingan nasionalnya tetapi juga untuk seluruh kawasan ASEAN. Sebagai negara yang memiliki pengalaman dan keahlian dalam bidang keamanan siber, Malaysia telah banyak berkontribusi dalam

pengembangan kebijakan dan strategi di tingkat regional. Salah satu inisiatif yang diusulkan oleh Malaysia adalah pembentukan pusat penanggulangan insiden siber regional, yang akan berfungsi sebagai hub untuk berbagi informasi dan koordinasi dalam menangani insiden siber (Malaysia Cyber Security Strategy, 2020).

Selain itu, Malaysia juga aktif dalam menyelenggarakan berbagai forum dan seminar yang melibatkan para ahli dan pemangku kepentingan dari negara-negara ASEAN. Contohnya, pada tahun 2019, Malaysia menjadi tuan rumah ASEAN Cybersecurity Conference yang dihadiri oleh perwakilan dari berbagai negara anggota. Dalam konferensi tersebut, dibahas berbagai isu terkait keamanan siber, termasuk tantangan yang dihadapi oleh masing-masing negara dan langkah-langkah yang dapat diambil untuk meningkatkan kolaborasi (ASEAN Cybersecurity Conference, 2019).

Partisipasi Malaysia dalam ACCF juga mencakup pengembangan kapasitas dan pelatihan bagi para profesional keamanan siber di seluruh ASEAN. Melalui program-program pelatihan dan workshop, Malaysia berupaya untuk meningkatkan keterampilan dan pengetahuan para praktisi keamanan siber di kawasan ini. Hal ini sangat penting mengingat banyaknya serangan siber yang dilakukan oleh aktor-aktor yang terorganisir dan memiliki sumber daya yang besar.

Lebih lanjut, Interpol (2022) dalam laporan terkait operasi penanggulangan kejahatan siber di ASEAN menekankan pentingnya kerja sama antar-negara, yang didukung oleh peran proaktif Malaysia. Malaysia

tidak hanya memberikan kontribusi dalam bentuk sumber daya dan keahlian, tetapi juga memfasilitasi berbagai program pelatihan dan peningkatan kapasitas bagi negara-negara anggota. Selain itu, laporan "Sibercrime and Its Impact in Southeast Asia" oleh United Nations Office on Drugs and Crime (UNODC) (2021) mencatat bahwa kolaborasi erat dalam forum ini telah menghasilkan penurunan signifikan insiden kejahatan siber di kawasan, berkat koordinasi strategis yang dipimpin oleh aktor-aktor utama seperti Malaysia. Kesimpulannya, melalui partisipasi aktif dan strategis dalam ASEAN Cybersecurity Cooperation Forum, Malaysia telah membuktikan dirinya sebagai pemimpin dalam upaya kolektif untuk mencapai stabilitas dan keamanan siber di Asia Tenggara.

Dari hasil penelitian yang telah dilakukan, peneliti telah meneliti studi sebelumnya mengenai peran Malaysia dalam menangani kejahatan siber di kawasan ASEAN. Penelitian yang dilakukan oleh Nugraha (2023) menunjukkan bahwa kerja sama dalam Strategi Kerja sama Keamanan Siber ASEAN telah memberikan dampak yang signifikan terhadap keamanan siber di wilayah tersebut, terutama di Indonesia. Penelitian ini menekankan pentingnya kerja sama regional dalam menghadapi ancaman siber yang semakin kompleks. Selain itu, penelitian yang dilakukan oleh Laksmono dan Fauzi (2024) menggambarkan bagaimana diplomasi pertahanan, melalui forum seperti Pertemuan Menteri Pertahanan ASEAN (ADMM), memfasilitasi koordinasi antar negara untuk mengatasi ancaman-ancaman termasuk terorisme. Meskipun fokus penelitian mereka lebih pada ancaman

terorisme, metodologi yang digunakan memberikan wawasan penting tentang efektivitas kerja sama multilateral. Meskipun topik kedua penelitian tersebut sedikit berbeda, namun keduanya menekankan pentingnya kerja sama regional dalam menghadapi ancaman keamanan non-tradisional. Namun, penelitian ini berbeda dengan penelitian sebelumnya karena lebih memfokuskan perhatian pada peran khusus Malaysia, bukan hanya dalam konteks kontribusi bersama, tetapi juga sebagai pemimpin inisiatif keamanan siber di forum ASEAN.

Dalam analisis lebih lanjut, penting untuk mencatat bagaimana penelitian sebelumnya menyoroti berbagai aspek dari peran kolektif negara-negara ASEAN dalam menangani kejahatan siber. Penelitian yang dilakukan oleh Nugraha seringkali menjadi referensi utama, dengan menampilkan data empiris mengenai dampak strategi keamanan siber terhadap stabilitas keamanan di wilayah tersebut. Dalam konteks ini, Malaysia muncul sebagai pemain utama yang menunjukkan kepemimpinan strategis dan kontribusi yang signifikan dalam memfasilitasi program-program peningkatan kapasitas dan pelatihan. Sementara itu, penelitian yang dilakukan oleh Laksmono dan Fauzi melengkapi konteks dengan menggambarkan bagaimana forum seperti ADMM dapat berperan sebagai platform efektif dalam kebijakan pertahanan terhadap ancaman lintas negara. Meskipun demikian, aspek spesifik dari peran Malaysia dalam mendorong keamanan siber di ASEAN belum banyak dieksplorasi dalam penelitian sebelumnya. Oleh karena itu, penelitian ini bertujuan untuk mengisi celah tersebut dengan menjelaskan secara detail

bagaimana langkah-langkah proaktif dan strategis Malaysia berhasil mempengaruhi dinamika keamanan siber di ASEAN secara keseluruhan, menjadikannya pemangku kepentingan utama dalam menciptakan ekosistem keamanan siber yang lebih kuat.

Dengan demikian, Penelitian ini bertujuan untuk menyelidiki dan menganalisis secara mendalam bentuk kerja sama dan peran strategis Malaysia dalam ASEAN Cybersecurity Cooperation Forum dalam upaya melawan kejahatan siber di kawasan ASEAN. Diketahui bahwa Malaysia memiliki peran penting sebagai pemimpin inisiatif keamanan siber di forum ASEAN, namun penelitian ini ingin memberikan penjelasan yang lebih komprehensif mengenai kontribusi nyata Malaysia yang belum terungkap dalam penelitian sebelumnya. Kebermaknaan penelitian ini terletak pada kemampuannya untuk melengkapi literatur yang ada dan memperkaya pemahaman tentang strategi dan kebijakan keamanan siber regional, terutama dalam konteks peran negara anggota utama seperti Malaysia. Dengan demikian, urgensi penelitian ini adalah untuk memahami dan memanfaatkan strategi Malaysia dalam memperkuat ekosistem keamanan siber di ASEAN. Dengan mengungkap langkah-langkah proaktif Malaysia, diharapkan hasil penelitian ini dapat membantu pembentukan kerangka kerja kolaboratif yang lebih solid dan memberikan wawasan berharga bagi pembuat kebijakan siber di tingkat regional. Penelitian ini tidak hanya berkontribusi dalam menangani kejahatan siber secara kolektif, tetapi juga memperkuat posisi Malaysia sebagai pemangku kepentingan utama dalam keamanan siber ASEAN.

Diharapkan peningkatan stabilitas dan keamanan siber yang berkelanjutan dapat memberikan manfaat bagi negara-negara anggota ASEAN dalam menghadapi ancaman siber yang semakin kompleks.

penelitian ini juga bertujuan untuk mengkaji peran Malaysia dalam ASEAN Cybersecurity Cooperation Forum, serta mengevaluasi kontribusi nyata yang diberikan oleh Malaysia dalam upaya menanggulangi kejahatan siber di kawasan ini. Studi ini diharapkan dapat memberikan wawasan baru mengenai dinamika kerja sama keamanan siber di ASEAN dan memicu diskusi lebih lanjut tentang pendekatan terbaik dalam menghadapi tantangan siber di era digital.

## B. Batasan dan Rumusan Masalah

Dalam penelitian ini, terdapat beberapa batasan yang diterapkan agar fokus penelitian lebih jelas dan hasil analisis lebih mendalam. Penelitian ini akan difokuskan pada wilayah ASEAN, dengan fokus utama pada kontribusi Malaysia dalam ASEAN Cybersecurity Cooperation Forum, tanpa membahas kebijakan atau kerja sama keamanan siber di luar ASEAN. Penelitian akan difokuskan pada periode 5 tahun terakhir (misalnya 2018-2023) untuk melihat perkembangan terkini dan peran Malaysia dalam forum kerja sama tersebut. Penelitian hanya akan membahas kebijakan, inisiatif, dan langkah-langkah yang diambil oleh Malaysia dalam kapasitasnya sebagai anggota ASEAN Cybersecurity Cooperation Forum untuk mengatasi kejahatan siber, tanpa memasukkan detail teknis operasional dari upaya penegakan hukum terhadap pelaku kejahatan siber. Penelitian ini tidak akan membahas aspek

teknologi atau teknis dalam mendeteksi dan menangani serangan siber, melainkan berfokus pada peran kebijakan, kerja sama regional, dan aspek diplomatik yang dijalankan oleh Malaysia dalam mendukung keamanan siber di ASEAN.Berikut rumusan masalah yang diangkat oleh penulis:

1. Bagaimana peran Malaysia dalam ASEAN Cybersecurity Cooperation Forum dalam menanggulangi kejahatan siber di ASEAN?
2. Bagaimana kontribusi Malaysia dalam ASEAN Cybersecurity Cooperation Forum berdampak terhadap upaya penanggulangan kejahatan siber di kawasan ASEAN?

## C. Tujuan dan Kegunaan penelitian

Berdasarkan rumusan masalah diatas,maka tujuan dari penelitian ini sebagai berikut:

1. Untuk menganalisis peran Malaysia dalam ASEAN Cybersecurity Cooperation Forum dalam menanggulangi kejahatan siber di ASEAN.
2. Untuk Mengetahui kontribusi Malaysia dalam ASEAN Cybersecurity Cooperation Forum berdampak terhadap upaya penanggulangan kejahatan siber di kawasan ASEAN

## D. Manfaat penelitian

Adapun manfaat dan kegunaan dari penelitian yang dilakukan penulis adalah sebagai berikut :

a. Manfaat Teoritis dari penelitian ini adalah untuk memberikan sumbangan dalam pemahaman tentang peran Malaysia dalam ASEAN Cybersecurity

Cooperation Forum dalam menanggulangi kejahatan siber di ASEAN. Dengan adanya penelitian ini, diharapkan dapat memberikan pemahaman yang lebih mendalam tentang bagaimana Malaysia berperan dalam forum tersebut dan bagaimana hal tersebut dapat berdampak pada upaya penanggulangan kejahatan siber di kawasan ASEAN secara keseluruhan. Selain itu, penelitian ini juga diharapkan dapat memberikan sumbangan dalam pengembangan teori-teori terkait keamanan siber dan kerja sama regional dalam menanggulangi ancaman siber di tingkat ASEAN.

b. Manfaat Praktis dari penelitian ini adalah untuk memberikan informasi yang bermanfaat bagi pihak terkait, seperti pemerintah Malaysia, ASEAN Cybersecurity Cooperation Forum, dan lembaga terkait lainnya, untuk meningkatkan kerja sama dalam menanggulangi kejahatan siber di kawasan ASEAN. Dengan mengetahui kontribusi Malaysia dalam forum tersebut, diharapkan dapat memperkuat kerja sama antar negara dalam menghadapi ancaman siber yang semakin kompleks. Selain itu, hasil penelitian ini juga dapat menjadi pedoman bagi pihak terkait dalam merumuskan kebijakan dan strategi dalam meningkatkan keamanan siber di tingkat regional.

## E. Kerangka Konseptual

### 1. Konsep Keamanan siber

Perlindungan sistem informasi dari ancaman digital, seperti akses ilegal, kerusakan, dan gangguan, dikenal sebagai keamanan siber. Dalam era

digital saat ini, keamanan siber menjadi sangat penting karena meningkatnya ancaman terhadap data dan infrastruktur digital yang mendukung berbagai aktivitas ekonomi dan sosial. Keamanan siber tidak hanya terkait dengan perangkat keras dan lunak, tetapi juga mencakup kebijakan dan prosedur yang dirancang untuk melindungi data dan jaringan. Oleh karena itu, upaya keamanan siber melibatkan tindakan pencegahan, deteksi, dan respons terhadap ancaman siber yang dapat merusak informasi.

Dengan perkembangan dunia digital yang terus berubah, ancaman siber menjadi semakin kompleks, sehingga keamanan siber harus dapat beradaptasi dengan cepat terhadap taktik peretas yang terus berkembang. Strategi keamanan yang responsif dan proaktif diperlukan untuk mengidentifikasi ancaman potensial sebelum terjadi eksploitasi serta merespons insiden keamanan dengan cepat dan efektif. Adaptasi ini melibatkan pembaruan sistem keamanan secara berkala, edukasi pengguna, dan pengembangan teknologi yang lebih aman. Dengan demikian, keamanan siber harus terus berkembang untuk menghadapi ancaman yang ada.

Selain itu, keamanan siber bukan hanya tanggung jawab individu atau organisasi, tetapi juga memerlukan kerja sama lintas batas, baik di tingkat nasional maupun internasional, untuk menciptakan lingkungan digital yang aman. Kerja sama ini melibatkan pertukaran informasi tentang ancaman terbaru, praktik terbaik, dan koordinasi dalam menghadapi serangan siber yang besar. Pendekatan kolaboratif ini memungkinkan negara dan organisasi untuk membangun sistem pertahanan siber yang lebih kuat dan efisien. Oleh

karena itu, keamanan siber memiliki peran penting dalam menjaga stabilitas dan integritas ekosistem digital global.

Selanjutnya, pendekatan keamanan siber juga membutuhkan kesadaran dan partisipasi semua pengguna teknologi. Edukasi dan kesadaran tentang pentingnya praktik keamanan siber yang baik merupakan faktor kunci dalam penerapan keamanan yang efektif. Pengguna teknologi perlu memahami risiko yang terkait dengan penggunaan internet dan menerapkan praktik aman seperti pengelolaan kata sandi yang kuat dan waspada terhadap phishing. Dengan meningkatkan kesadaran masyarakat tentang keamanan siber, diharapkan bahwa mereka akan lebih waspada terhadap ancaman siber dan dapat berperan aktif dalam menjaga keamanan informasi pribadi dan organisasi.

Keamanan siber memiliki fungsi krusial dalam melindungi data dan informasi dari ancaman kejahatan di dunia maya (Fauzi et al., 2023). Perlindungan ini menjadi semakin penting seiring dengan meningkatnya serangan siber yang dapat merugikan individu dan organisasi. Fungsi utama keamanan siber adalah menjaga kerahasiaan, integritas, dan ketersediaan data agar tetap tidak terakses oleh pihak yang tidak berwenang. Dalam lingkungan digital yang terus berkembang, fungsi ini memastikan bahwa sistem dan jaringan komputer dapat beroperasi dengan aman tanpa gangguan eksternal. Keamanan siber juga memainkan peran penting dalam mendeteksi dan menanggapi insiden siber, sehingga meminimalkan dampak negatif yang mungkin ditimbulkan. Penguatan keamanan ini diperlukan agar data tetap

aman dan proses bisnis dapat berjalan lancar tanpa hambatan dari ancaman siber.

Selanjutnya, keamanan siber berfungsi untuk mengidentifikasi potensi risiko yang mengancam sistem informasi. Dengan menggunakan berbagai alat dan teknik, pakar keamanan dapat mendeteksi celah keamanan dan mengatasinya sebelum dapat dieksploitasi oleh penyerang. Misalnya, evaluasi rutin terhadap sistem dan jaringan membantu dalam menemukan dan memperbaiki kelemahan sebelum mereka digunakan untuk pengambilan data secara tidak sah. Keterkaitan antara identifikasi dan pencegahan ancaman ini menegaskan pentingnya peran keamanan siber dalam melindungi infrastruktur digital. Selain itu, upaya ini diperlukan untuk memastikan bahwa langkah-langkah keamanan yang diterapkan dapat beradaptasi dengan ancaman yang terus berkembang.

Selain identifikasi ancaman, fungsi keamanan siber juga mencakup mitigasi risiko dengan menerapkan kebijakan keamanan yang ketat. Ini mencakup penggunaan enkripsi, autentikasi dua faktor, dan firewall untuk mengamankan sistem. Kebijakan ini dirancang untuk membatasi akses hanya kepada pengguna yang sah, mengurangi kemungkinan terjadi pelanggaran data. Mitigasi tersebut harus selaras dengan standar industri agar keefektifannya terjamin. Komponen penting lainnya adalah pendidikan dan pelatihan bagi pengguna untuk meningkatkan kesadaran akan praktik keamanan yang baik. Pelatihan ini berfungsi untuk meminimalisasi risiko

kesalahan manusia yang sering menjadi penyebab utama terjadinya pelanggaran siber.

Implementasi dari strategi dan kebijakan keamanan juga mendukung keberlangsungan operasional organisasi. Dengan adanya sistem keamanan yang kuat, sistem dapat terus berfungsi selama terjadi ancaman siber kepada infrastruktur TI. Keandalan operasional ini krusial untuk menjaga kepercayaan pemangku kepentingan dan mencegah kerugian finansial atau reputasi. Keberlanjutan ini dicapai melalui keberlanjutan penilaian risiko secara berkala dan memperbarui kebijakan keamanan sesuai kebutuhan. Oleh karena itu, keamanan siber memainkan fungsi penting dalam menciptakan ekosistem digital yang aman dan berkelanjutan di tengah dinamika ancaman siber yang terus berubah.

Konsep 'Ruang Lingkup' dalam konteks keamanan siber memerlukan pemahaman yang mendalam terhadap berbagai faktor yang memengaruhinya. Keamanan siber tidak hanya melibatkan langkah-langkah pencegahan terhadap akses yang tidak sah, tetapi juga melibatkan upaya untuk mendeteksi, menanggulangi, dan memulihkan sistem dari gangguan atau serangan digital. Langkah pencegahan ini mencakup penggunaan firewall, enkripsi data, dan pelatihan keamanan bagi pengguna sebagai langkah awal dalam membangun pertahanan yang kuat. Sementara itu, deteksi memerlukan sistem pemantauan yang dapat mengidentifikasi ancaman secara real-time. Memahami konsep ini penting untuk memastikan bahwa strategi keamanan yang diadopsi dapat diimplementasikan dengan efektif.

Kesuksesan dalam menerapkan keamanan siber sangat bergantung pada ruang lingkup yang jelas dan komprehensif. Ruang lingkup ini mencakup berbagai tingkat keamanan, mulai dari kebijakan organisasi hingga teknologi spesifik yang digunakan untuk melindungi infrastruktur digital. Kebijakan organisasi penting untuk memastikan bahwa seluruh proses operasional berada dalam pengawasan yang ketat, termasuk prosedur keamanan yang harus diikuti oleh semua anggota organisasi. Di sisi lain, teknologi spesifik seperti software deteksi ancaman dan sistem manajemen insiden harus selalu diperbarui agar siap menghadapi ancaman terbaru. Dengan demikian, ruang lingkup yang terdefinisi dengan baik akan meningkatkan kesiapsiagaan dan respons terhadap serangan siber.

Selain itu, ruang lingkup keamanan siber juga memperhatikan kerangka hukum yang berkaitan dengan hak dan tanggung jawab dalam dunia maya. Aspek ini mencakup peraturan dan regulasi yang membantu mengawasi aktivitas digital dan menetapkan batasan hukum untuk mencegah tindakan kejahatan. Pemahaman tentang hukum internasional terkait serangan siber dan kerja sama antar negara dalam menanggapi serangan tersebut juga termasuk dalam ruang lingkup yang harus diperhatikan. Hal ini tidak hanya melindungi data yang dimiliki, tetapi juga mendorong integrasi dan kerja sama antar badan pengawas yang relevan, memperkuat pertahanan dan penggunaan teknologi digital secara etis dan bertanggung jawab.

Terakhir, ruang lingkup keamanan siber harus mencakup upaya pendidikan dan peningkatan kesadaran bagi pengguna akhir. Tanpa

pemahaman yang baik tentang praktik keamanan yang benar, banyak langkah pencegahan dapat menjadi tidak efektif karena kesalahan manusia. Oleh karena itu, pelatihan dan sosialisasi mengenai keamanan siber perlu dilakukan secara rutin sebagai bagian dari strategi keamanan yang komprehensif. Ini termasuk pengetahuan tentang cara mengenali ancaman online, langkah-langkah dalam menjaga kerahasiaan password, dan cara merespons saat menghadapi insiden Cybersecurity. Dengan demikian, ruang lingkup edukasi ini menjadi faktor kunci dalam membentuk budaya keamanan yang lebih baik di era digital saat ini.

Elemen-elemen kunci dalam karakteristik keamanan siber merupakan fondasi utama dalam melindungi data dan informasi dari ancaman dunia maya. Menurut penelitian oleh Fauzi dan rekan (2023), keamanan siber meliputi berbagai pengaturan teknologi dan kontrol yang dirancang untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi. Kerahasiaan bertujuan untuk membatasi akses data hanya kepada pihak yang berwenang, sementara integritas memastikan bahwa data tidak dapat diubah oleh pihak yang tidak berwenang. Ketersediaan, sebagai elemen ketiga, menjamin bahwa sistem dan data tetap dapat diakses dan digunakan saat diperlukan.

Selain itu, pengelolaan risiko juga merupakan karakteristik penting dalam keamanan siber. Organisasi harus mengidentifikasi, menilai, dan merespons risiko yang dapat mengancam sistem informasi mereka. Pengelolaan risiko membantu dalam menentukan strategi untuk mengurangi dampak potensi ancaman. Memahami dan mengurangi risiko ini membantu

menciptakan lingkungan yang lebih aman dan memastikan kelangsungan operasional. Langkah-langkah mitigasi melibatkan kebijakan, prosedur, dan teknologi untuk mengurangi kemungkinan insiden keamanan.

Selain itu, pentingnya pelatihan dan kesadaran keamanan bagi pengguna juga menjadi karakteristik yang menonjol. Faktor manusia sering menjadi titik lemah dalam keamanan siber. Pengguna yang terlatih dan sadar akan pentingnya praktik keamanan memiliki peran penting dalam mencegah pelanggaran keamanan siber. Program pelatihan harus mencakup topik seperti ancaman umum, cara mengidentifikasinya, dan protokol pelaporan insiden. Investasi dalam pendidikan keamanan siber merupakan langkah strategis dalam memperkuat keamanan organisasi.

Terakhir, penerapan teknologi canggih seperti enkripsi dan firewall juga merupakan karakteristik vital dalam menjaga keamanan siber. Teknologi ini berperan sebagai penghalang untuk melindungi data dari akses tidak sah dan serangan luar. Enkripsi mengamankan data dengan mengkodekan informasi sehingga hanya dapat dibaca oleh pihak yang memiliki kunci dekripsi. Firewall berfungsi sebagai penjaga pintu yang memfilter lalu lintas jaringan untuk memastikan keamanan data. Dengan mengintegrasikan teknologi ini, organisasi dapat memperkuat mekanisme perlindungan dan mempertahankan kepercayaan pengguna terhadap keamanan sistem informasi yang mereka kelola.

**2. Konsep Kerja sama Internasional**

Kolaborasi antar negara untuk mencapai tujuan bersama melalui koordinasi dan kolaborasi yang terstruktur dapat diartikan sebagai kerja sama

internasional. Dalam konteks ini, kerja sama internasional melibatkan pertukaran informasi, sumber daya, dan keahlian untuk mengatasi masalah global yang kompleks. Pentingnya saling pengertian dan kepercayaan antar negara untuk menciptakan lingkungan yang kondusif bagi stabilitas dan pembangunan dunia ditekankan dalam definisi ini. Menurut penelitian terbaru, kerja sama internasional sering melibatkan jaringan lembaga untuk meningkatkan efisiensi dan efektivitas dalam mencapai tujuan yang telah disepakati.

Kerangka kerja sama internasional berkembang seiring dengan kompleksitas tantangan global yang semakin meningkat, membutuhkan sinergi dan konsensus yang lebih luas. Sinergi ini memungkinkan negara-negara untuk menggabungkan kekuatan mereka dalam menghadapi isu-isu seperti keamanan, ekonomi, kesehatan, dan lingkungan. Keterlibatan berbagai aktor, baik pemerintah maupun non-pemerintah, dalam kerangka kerja sama internasional memperkuat dinamika ini dan menunjukkan bahwa interaksi multilateral menjadi kunci dalam dinamika global saat ini.

Ruang lingkup kerja sama internasional semakin luas dengan melibatkan berbagai sektor dalam implementasinya. Hal ini memungkinkan integrasi perspektif yang berbeda dan lebih beragam dalam strategi dan solusi yang diterapkan. Kolaborasi dalam bidang teknologi dan informasi, sebagai contoh, telah terbukti mendorong inovasi yang signifikan, meningkatkan kemampuan negara untuk menghadapi tantangan seperti keamanan siber. Inovasi dalam teknologi memberikan peluang baru untuk pertukaran

informasi yang lebih cepat dan efisien, serta memungkinkan penanganan masalah dengan pemahaman yang lebih mendalam dan terukur.

Keberhasilan kerja sama internasional sangat tergantung pada komitmen dan kesetiaan para partisipan terhadap norma dan prinsip yang telah disepakati bersama. Komitmen ini mencakup penghormatan terhadap kedaulatan negara, prinsip kesetaraan, dan keadilan dalam kerja sama. Dengan mematuhi standar tersebut, negara-negara dapat memastikan bahwa kerja sama yang dibangun memberikan manfaat yang merata bagi seluruh peserta. Prinsip-prinsip ini menjadi pedoman dalam proses negosiasi dan implementasi, memastikan bahwa semua pihak memiliki suara dan dapat berkontribusi aktif dalam kerangka kerja sama tersebut.

Pentingnya landasan teori dalam sebuah skripsi adalah untuk menjelaskan konsep yang digunakan dalam penelitian. Menurut Yusniah et al. (2023), kerja sama internasional memiliki peran penting dalam memperkuat hubungan antar negara melalui pertukaran informasi dan sumber daya. Kerja sama ini juga memungkinkan pertukaran pengetahuan dan teknologi yang dapat memacu perkembangan suatu negara serta meningkatkan efisiensi dalam mencapai tujuan bersama. Dalam konteks yang sama, kerja sama internasional juga memungkinkan negara-negara untuk saling melengkapi sumber daya dan keahlian guna mencapai perkembangan yang lebih baik.

Keberlanjutan kerja sama internasional menjadi kunci dalam menciptakan hubungan yang harmonis dan stabil. Hal ini memastikan bahwa

manfaat dari kerja sama tidak hanya dirasakan secara jangka pendek tetapi juga memberikan dampak positif yang berkelanjutan. Contohnya, dalam kerja sama perpustakaan internasional, keterlibatan berkelanjutan antara perpustakaan dari berbagai negara dapat meningkatkan akses terhadap sumber daya informasi secara global, yang pada akhirnya berkontribusi pada peningkatan kualitas pelayanan.

Kerja sama internasional juga berperan penting dalam membangun kapasitas kelembagaan. Dengan adanya kerja sama ini, institusi di berbagai negara dapat berbagi pengetahuan dan praktik terbaik untuk meningkatkan kemampuan kelembagaan secara keseluruhan. Dalam konteks perpustakaan, kerja sama internasional memungkinkan berkembangnya sistem manajemen informasi yang lebih baik untuk meningkatkan aksesibilitas dan kualitas pelayanan.

Terakhir, kerja sama internasional berperan sebagai landasan untuk membangun jaringan strategi kolaboratif yang solid. Jaringan ini memungkinkan pertukaran informasi dan ide-ide inovatif untuk menghasilkan solusi yang lebih kreatif dan efektif dalam mengatasi tantangan global. Dengan strategi kolaboratif yang kuat, negara-negara dapat mencapai tujuan kolektif mereka dengan lebih efisien dan efektif, serta memperkuat kapasitas individual maupun kelembagaan negara-negara yang terlibat.

Keberadaan cakupan dalam kerja sama internasional memiliki tujuan untuk memahami batasan dan fokus dari kolaborasi yang dilakukan. Sebagai contoh, dalam kerja sama antara perpustakaan Indonesia-Malaysia, cakupan

kerja sama ini mencakup pertukaran informasi, sumber daya perpustakaan, dan pengembangan kapasitas pustakawan dalam konteks internasionalisasi pendidikan dan ilmu pengetahuan. Melalui kerja sama internasional ini, kedua negara dapat bersama-sama mengidentifikasi dan mengatasi kebutuhan serta tantangan yang dihadapi. Oleh karena itu, cakupan kerja sama menjadi faktor krusial dalam memastikan efektivitas dan keberlanjutan dari upaya yang dilakukan.

Selain itu, cakupan kerja sama internasional juga dapat diperluas dengan mempertimbangkan berbagai dimensi yang terlibat, seperti aspek hukum, politik, ekonomi, dan sosial-budaya yang mempengaruhi interaksi antarnegara. Dalam konteks perpustakaan, hal ini melibatkan regulasi hak cipta, akses informasi, dan standar profesional. Kerja sama juga dapat melibatkan penyelenggaraan seminar, lokakarya, dan pelatihan untuk meningkatkan kompetensi pustakawan. Dengan pemahaman ini, kerja sama tidak hanya memberikan keuntungan bagi institusi yang terlibat, tetapi juga berkontribusi pada pengembangan ilmu pengetahuan secara regional dan internasional.

Kemampuan institusi dalam menghadapi dinamika global juga memengaruhi cakupan kerja sama internasional. Teknologi informasi dan komunikasi (TIK) memiliki peran penting dalam memperluas kerja sama. Adopsi teknologi terkini memungkinkan pertukaran informasi yang lebih cepat dan efisien, membuka peluang kolaborasi lintas negara. Evaluasi berkelanjutan dari cakupan kerja sama internasional juga penting untuk

mengevaluasi efektivitas kerja sama dan mengidentifikasi area yang perlu ditingkatkan. Dengan evaluasi yang rutin, institusi dapat menyesuaikan cakupan kerja sama agar tetap relevan dengan perkembangan global. Fleksibilitas dan responsivitas terhadap perubahan menjadi kunci dalam menjaga kerja sama yang efektif dan berkelanjutan.

Karakteristik kerja sama internasional dapat dilihat dari beberapa aspek yang menjadi dasar keberhasilannya. Pertama, kerja sama internasional dicirikan oleh adanya kesepakatan resmi antara pihak-pihak yang terlibat. Kesepakatan ini umumnya dicatat dalam bentuk perjanjian atau memorandum yang mencakup tujuan, cakupan, serta hak dan kewajiban masing-masing pihak. Aspek kesepakatan ini sangat penting untuk memastikan bahwa semua pihak memiliki pemahaman yang jelas tentang tujuan dan kontribusi mereka dalam kerja sama tersebut. Keterbukaan dalam kesepakatan ini menjadi dasar bagi kelangsungan dan kesuksesan kerja sama di tingkat internasional.

Selanjutnya, karakteristik lain dari kerja sama internasional adalah adanya komunikasi dan koordinasi yang efisien antara pihak-pihak yang terlibat. Komunikasi yang efektif menjadi kunci untuk mengatasi perbedaan yang mungkin timbul akibat latar belakang budaya dan sistem hukum yang berbeda. Koordinasi juga diperlukan untuk menyelaraskan berbagai kegiatan dan inisiatif yang dilakukan dalam konteks kerja sama ini. Efektivitas komunikasi dan koordinasi dapat meningkatkan pemahaman dan kepercayaan antara pihak-pihak, sehingga mengurangi potensi konflik dan

meningkatkan sinergi. Sinergi yang tercipta dari komunikasi yang baik akan memperkuat pencapaian tujuan kerja sama.

Karakteristik berikutnya yang penting adalah fleksibilitas dalam pelaksanaan kerja sama. Fleksibilitas ini penting untuk mengakomodasi perubahan yang mungkin terjadi selama kerja sama berlangsung, baik perubahan internal maupun eksternal. Situasi global yang dinamis menuntut kerja sama internasional untuk dapat beradaptasi dengan cepat terhadap perubahan yang terjadi. Oleh karena itu, kebijakan dan strategi yang diterapkan dalam kerja sama tersebut harus memiliki unsur fleksibilitas agar tetap relevan dan efektif. Fleksibilitas ini memungkinkan kerja sama untuk tetap berjalan meskipun menghadapi tantangan yang tidak terduga.

Terakhir, keberlanjutan kerja sama internasional juga dipengaruhi oleh komitmen jangka panjang dari semua pihak yang terlibat. Komitmen ini tidak hanya ditunjukkan melalui partisipasi aktif dalam setiap kegiatan, tetapi juga melalui penyediaan sumber daya yang memadai untuk mendukung kelangsungan kerja sama. Penyediaan sumber daya dapat berupa pendanaan, tenaga ahli, atau teknologi yang diperlukan untuk mencapai tujuan bersama. Keberlanjutan ini akan memastikan bahwa kerja sama mampu memberikan kontribusi yang nyata dan bermanfaat bagi semua pihak dalam jangka panjang. Dengan komitmen yang kuat, kerja sama internasional dapat bertahan menghadapi berbagai tantangan global yang ada.

Indikator dalam kerja sama internasional memiliki peran yang penting dalam mengevaluasi efektivitas dan keberhasilan kesepakatan antar negara.

Indikator ini umumnya mencerminkan beberapa aspek utama, seperti tingkat partisipasi negara anggota, keselarasan kebijakan, dan pencapaian tujuan bersama yang telah disepakati. Selain itu, indikator dapat digunakan untuk menilai kontribusi masing-masing negara terhadap upaya kolektif. Keberhasilan evaluasi kerja sama internasional bergantung pada pemilihan indikator yang tepat yang mencerminkan kondisi sebenarnya dari kerja sama tersebut.

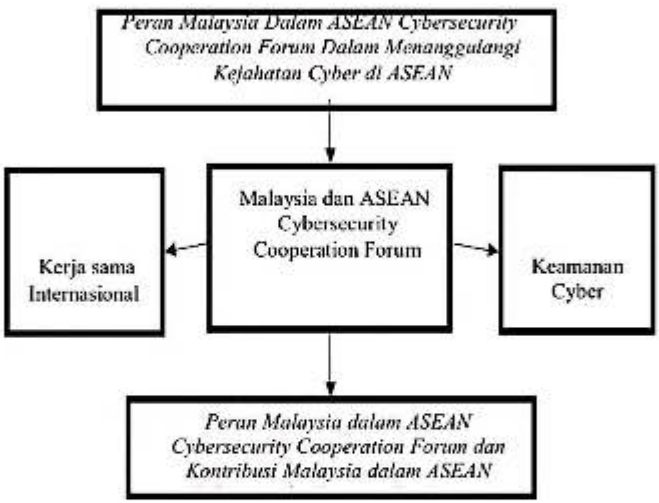
Konsistensi dalam penerapan indikator menjadi kunci sukses kerja sama internasional. Penerapan yang konsisten memastikan bahwa pengukuran yang dihasilkan dapat diandalkan dan digunakan sebagai dasar pengambilan keputusan. Konsistensi ini melibatkan penyesuaian indikator sesuai dengan perubahan dinamika kerja sama internasional. Penyelarasan indikator dengan tujuan kerja sama juga sangat penting untuk memastikan relevansi dan keberhasilan evaluasi.

Indikator dalam kerja sama internasional bukan hanya sebagai alat ukur, tetapi juga sebagai instrumen pengendalian yang memberikan arahan pengembangan hubungan antar negara. Indikator yang tepat dapat mengidentifikasi area yang memerlukan perbaikan dan merumuskan strategi untuk mengatasi tantangan yang ada. Sebagai instrumen pengendalian, indikator memfasilitasi pencapaian tujuan dengan memastikan bahwa kerja sama diukur dan dimonitor secara sistematis. Dengan demikian, indikator menjadi bagian integral dari proses evaluasi yang mendukung peningkatan kualitas kerja sama internasional secara berkelanjutan.

## F. Skema Kerangka Konseptual Pembahasan

Penulis mengaplikasikan alur berpikir dalam penyusunan penelitian ini yang dapat digambarkan seperti bagan berikut.

**Bagan 1. Alur Berpikir**




Dalam penelitian ini terdapat dua variabel yakni variabel independen dan variabel dependen. Variabel independen atau biasa disebut variabel bebas ini merujuk pada faktor yang memengaruhi atau menjadi penyebab munculnya variabel dependen. Sementara variabel dependen atau dikenal sebagai variabel terikat berperan sebagai reaksi atau faktor hasil yang dipengaruhi oleh variabel independen. Dalam penelitian ini,Kejahatan Siber menjadi variabel dependen,peran malaysia dalam ASEAN Cybesecurity Cooperation Forum dalam menanggulangi kejahatan siber di ASEAN

menjadi variabel independen.

Berdasarkan bagan di atas, penulis menekankan yang di ukur untuk mengetahui peran Malaysia dalam ASEAN Sibersrcurity Cooperation Forum dalam menanggulangi kejahatan Siber di ASEAN yaitu menggunakan konsep kerja samainternasional dan keamanan siber yang akan diperluas dengan kebijakan internasional dan upaya kontribusi kedua negara.Peran Malaysia yang di ukur dalam penelitian ini adalah kebijakan dan regulasi keamanan siber untuk menanggulangi kasus kejahatan siber di ASEAN.

## G. Metode Penelitian

Terdapat struktur-struktur yang digunakan Penulis untuk menyusun penelitian ini agar dapat tersusun sesuai metodenya. Berikut ini akan dijelaskan mengenai struktur metode penelitian yang digunakan Penulis.

### 1. Tipe Penulisan

Tipe penelitian yang digunakan oleh Penulis yakni penelitian studi kasus dengan pendekatan kualitatif. Penelitian studi kasus bertujuan untuk meneliti suatuperistiwa yang sudah terjadi di mana fokus utamanya ialah untuk mengetahui semuahubungan dari variabel yang ada dalam peristiwa. Tujuan dasar dari penelitian studikasus ialah mengetahui penyebab suatu peristiwa bisa terjadi, terulang, dan kemudian berlangsung dalam jangka panjang di masyarakat.Melalui tipe penelitian ini, Penulis akan berusaha menjabarkan mengenai peran Malaysia dalam ASEAN Cybersecurity

Cooperation Forum dalam menanggulangi kejahatan siber di ASEAN sehingga akan diketahui faktor-faktor dan bentuk kerjasama apa yang di lakukan negara dan organisasi tersebut.

**2. Jenis Data**

Jenis data yang akan digunakan penulis pada proses penelitian ini adalah datasekunder. Data sekunder merupakan jenis data yang sudah ada atau data-data tersebut telah dikumpulkan oleh lembaga serta organisasi penyelidik sebelumnya. Data-data sekunder dapat diperoleh melalui buku, artikel, jurnal, dokumen resmi, Undang-Undang Negara, situs jejaring resmi, serta sumber elektronik yang memuatanalisis tentang kebijakan keamanan siber dan implementasinya di Malaysia dan Perjanjian bilateral atau multilateral yang mencakup aspek keamanan siber.

**3. Teknik Pengumpulan data**

Pada penelitian ini, Penulis menggunakan teknik pengumpulan data studi kepustakaan (*library research*) yakni dokumen atau catatan dari peristiwa yang telah berlalu, baik dalam bentuk tulisan, gambar, atau karya dari seseorang yang tentunya relevan dengan topik yang diangkat oleh Peneliti.

**4. Teknik Analisis Data**

Pendekatan yang digunakan Penulis untuk menganalisis data ialah dengan menggunakan teknik kualitatif deskriptif. Analisis data kualitatif merupakan metode yang digunakan untuk mengkaji, menemukan, mendeskripsikan, dan memberikan kejelasan atas kualitas atau

keistimewaan dari pengaruh sosial yang tidak dapat dijelaskan, diukur, atau digambarkan melalui pendekatan kuantitatif (Saryono, 2010).

# BAB II

# TINJAUAN PUSTAKA

## A. Keamanan Siber

Keamanan siber, suatu konsep yang esensial dalam era digital, merujuk pada praktik melindungi sistem komputer dan jaringan dari ancaman digital yang mengganggu integritas, kerahasiaan, dan ketersediaan informasi. Konsep ini mencakup berbagai metode dan teknologi yang dirancang untuk melindungi data dari ancaman eksternal maupun internal (Susanto et al., 2023). Definisi keamanan siber meluas pada perlindungan infrastruktur teknologi informasi dari serangan digital yang dapat mengakibatkan pencurian data atau gangguan layanan vital. Dalam perspektif yang lebih spesifik, keamanan siber juga mencakup praktis-praktik seperti enkripsi data, pengendalian akses, serta pemantauan aktivitas jaringan secara berkala, yang semuanya bertujuan untuk meminimalisir risiko yang dihadapi oleh pengguna (Fauzi et al., 2023).

Penggunaan istilah keamanan siber sering kali dikaitkan dengan ancaman digital yang semakin berkembang, seperti malware, phishing, dan ransomware (Susanto et al., 2023). Ancaman-ancaman ini dapat menyebabkan kerugian finansial dan reputasi bagi individu maupun organisasi. Oleh karena itu, penting untuk mengimplementasikan strategi keamanan siber yang efektif demi melindungi aset digital. Strategi ini dapat mencakup investasi dalam teknologi keamanan terbaru dan peningkatan kesadaran akan pentingnya keamanan data di kalangan pengguna. Kesadaran tersebut menjadi kunci dalam memastikan bahwa

praktik keamanan siber diadopsi secara menyeluruh oleh seluruh lapisan pengguna teknologi (Fauzi et al., 2023).

Seiring dengan meningkatnya interkoneksi sistem informasi global, keamanan siber tidak hanya menjadi isu teknis, tetapi juga tantangan global yang memerlukan kerja sama internasional. Kerja sama ini bertujuan untuk berbagi informasi dan menciptakan lingkungan digital yang lebih aman (Transnasional & Perkasa, 2023). Dalam konteks ini, penting bagi negara-negara untuk membentuk aliansi guna menghadapi ancaman siber yang kian kompleks. Aliansi tersebut memungkinkan penegakan aturan dan standar yang disepakati bersama, sehingga mampu memperkuat pertahanan siber secara kolektif. Dengan demikian, kolaborasi internasional menjadi elemen krusial dalam taktik pengamanan siber yang efektif.

Perkembangan teknologi yang pesat menambah lapisan kompleksitas dalam praktik keamanan siber, mengingat tantangan yang dihadapi juga semakin canggih dan sulit untuk diprediksi. Oleh karenanya, penelitian dan pengembangan terus-menerus dalam bidang ini sangat diperlukan untuk mengantisipasi berbagai kemungkinan ancaman yang mungkin muncul di masa depan (Susanto et al., 2023).

Pentingnya keamanan siber dalam menjaga stabilitas dan keutuhan infrastruktur digital tidak dapat dipandang sebelah mata, mengingat dampaknya yang sangat luas terhadap sektor-sektor penting lainnya seperti ekonomi, politik, dan sosial. Oleh karena itu, pemahaman mendalam

tentang definisi dan ruang lingkup keamanan siber menjadi landasan dalam upaya pencegahan dan penanggulangan ancaman siber secara efektif.

Keamanan siber dalam era digital merupakan hal yang kompleks dan terus berkembang. Selain melindungi perangkat keras dan lunak, keamanan siber juga melibatkan perlindungan terhadap data individu dan organisasi dari ancaman di dunia maya. Keamanan siber mencakup menjaga kerahasiaan, integritas, dan ketersediaan informasi serta melibatkan aspek hukum, kebijakan, teknologi informasi, edukasi, dan pelatihan pengguna. Semakin terhubungnya sistem informasi membuat keamanan siber menjadi bagian penting dari manajemen risiko organisasi.

Kolaborasi antara pelaku industri, pemerintah, dan masyarakat diperlukan dalam mencegah dan menangani ancaman keamanan siber yang semakin kompleks dan transnasional. Kebijakan dan kerangka kerja internasional yang harmonis juga mendukung keamanan siber global. Aspek teknis keamanan siber mencakup berbagai alat dan metode untuk melindungi jaringan, sistem, dan data dari serangan siber dengan teknologi seperti kecerdasan buatan, pembelajaran mesin, dan enkripsi.

Pendidikan dan pelatihan keamanan siber penting untuk meningkatkan kesiapsiagaan manusia dalam menghadapi ancaman siber. Investasi dalam program pelatihan keamanan siber bertujuan untuk memberikan pengetahuan tentang ancaman potensial dan cara pencegahannya serta memperkuat budaya keamanan dalam organisasi.

Dengan pemahaman dan keterampilan yang memadai, pengguna akhir dapat menjadi pertahanan pertama melawan serangan siber yang semakin canggih. Keamanan siber tidak hanya melibatkan aspek teknis tetapi juga elemen manusia sebagai faktor penting.

Karakteristik keamanan siber memiliki aspek yang sangat penting dalam menjaga keamanan data dan sistem digital. Menurut penelitian oleh Susanto dan rekan (2023), keamanan siber pada era digital fokus pada tiga elemen utama: kerahasiaan, integritas, dan ketersediaan. Kerahasiaan bertujuan untuk melindungi informasi dari akses yang tidak sah, sementara integritas memastikan bahwa data tidak dapat diubah tanpa izin. Ketersediaan berarti bahwa sistem dan data harus dapat diakses oleh pengguna yang sah kapan pun diperlukan. Ketiga elemen ini sangat penting untuk memastikan bahwa keamanan siber dapat berfungsi dengan baik dalam berbagai situasi.

Fauzi dan tim (2023) juga menyoroti pentingnya respons yang cepat dan adaptif dalam keamanan siber. Respons ini mencakup identifikasi ancaman secara real-time dan penerapan tindakan mitigasi dengan cepat. Hal ini menunjukkan perlunya sistem yang dapat mendeteksi ancaman atau serangan lebih awal sebelum berdampak besar. Respons yang cepat ini juga mendukung kerahasiaan, integritas, dan ketersediaan data, karena dapat mencegah akses yang tidak sah dan memastikan layanan tetap tersedia. Oleh karena itu, kemampuan untuk beradaptasi juga merupakan faktor penting dalam memperkuat

karakteristik keamanan siber.

Selain itu, pembelajaran berbasis data juga menjadi bagian penting dalam meningkatkan efektivitas keamanan siber. Dengan menganalisis data dari berbagai ancaman dan serangan, pembelajaran ini dapat mengembangkan strategi perlindungan yang lebih canggih. Dengan mengotomatisasi proses analisis ini, sistem keamanan siber dapat meningkatkan deteksi dan respons terhadap ancaman. Contohnya, penggunaan kecerdasan buatan dan pembelajaran mesin dalam menganalisis data ancaman dapat membantu mengidentifikasi pola yang menunjukkan potensi serangan siber, sehingga dapat memberikan peringatan dini dan meningkatkan tindakan pencegahan yang diperlukan.

Parameter penting dalam keamanan siber adalah indikator yang digunakan untuk mengevaluasi efektivitas strategi perlindungan data dan infrastruktur digital. Menurut penelitian oleh Susanto dan timnya (2023), indikator tersebut meliputi aspek-aspek seperti deteksi serangan, respons terhadap insiden, dan pemulihan dari serangan. Deteksi serangan bertujuan untuk sistem dapat mengidentifikasi ancaman secara real-time dan mencegah dampak negatifnya (Susanto et al., 2023). Respons terhadap insiden menilai kecepatan dan ketepatan tindakan yang diambil saat terjadi pelanggaran keamanan, yang sangat penting untuk mengurangi risiko lebih lanjut. Sementara itu, pemulihan dari serangan mengukur efisiensi proses mengembalikan operasional normal setelah terjadi gangguan keamanan (Susanto et al., 2023). Indikator-indikator ini secara bersama-sama

memberikan gambaran menyeluruh tentang kesiapan dan ketahanan sistem terhadap ancaman siber.

Keberhasilan dalam menerapkan keamanan siber sangat tergantung pada pemahaman yang mendalam tentang indikator-indikator tersebut. Menurut Fauzi dan koleganya (2023), salah satu indikator penting adalah kemampuan analisis data, yang memungkinkan organisasi untuk mengidentifikasi pola serangan dan mengambil tindakan preventif secara proaktif. Analisis ini sering melibatkan penggunaan algoritma canggih dan teknologi machine learning untuk memproses data dalam jumlah besar guna mendeteksi anomali yang mungkin terlewat oleh sistem konvensional (Fauzi et al., 2023). Dengan demikian, pemahaman yang mendalam tentang pola ancaman dapat meningkatkan efisiensi sistem deteksi dan mengoptimalkan respons. Semakin baik kemampuan analisis ini diterapkan, semakin tinggi tingkat efektivitas keamanan yang dapat dicapai oleh suatu entitas.

Selain itu, indikator-indikator tersebut juga mencerminkan kebijakan dan prosedur yang diterapkan dalam manajemen keamanan informasi. Menurut Perkasa dan timnya, keberhasilan dalam manajemen keamanan siber memerlukan pembaruan reguler terhadap kebijakan dan evaluasi yang terencana (Perkasa, 2023). Kebijakan ini harus dirancang untuk memastikan bahwa semua pihak terlibat memahami peran mereka dalam menjaga keamanan data. Sebagai contoh, latihan simulasi serangan siber secara rutin adalah indikator lain yang membantu mengukur kesiapan

organisasi dalam menghadapi ancaman nyata. Indikator ini tidak hanya menguji keandalan sistem, tetapi juga mengukur kesiapan sumber daya manusia dalam merespons insiden. Dengan demikian, penilaian terhadap indikator-indikator ini memberikan wawasan berharga tentang kekuatan dan kelemahan sistem keamanan yang ada.

Terakhir, indikator kinerja keamanan siber juga berkaitan erat dengan teknologi yang digunakan, seperti penggunaan enkripsi dan autentikasi multifaktor. Enkripsi data merupakan elemen penting dari sistem keamanan modern, di mana enkripsi berperan sebagai lapisan terakhir untuk melindungi informasi sensitif dalam situasi kompromi sistem (Fauzi et al., 2023). Autentikasi multifaktor juga meningkatkan kompleksitas bagi penyerang dengan menambahkan lapisan verifikasi tambahan yang membatasi akses yang tidak sah. Indikator ini menyoroti pentingnya pendekatan berlapis dalam perlindungan dan menunjukkan bagaimana teknologi dapat digunakan sebagai alat utama untuk mengukur dan meningkatkan standar keamanan. Secara keseluruhan, indikator-indikator dalam keamanan siber bukan hanya sebagai alat ukur, tetapi juga memberikan arahan strategis bagi organisasi agar dapat terus beradaptasi dengan ancaman yang selalu berubah.

**B. Kerja sama Internasional**

Dalam bidang studi hubungan internasional, kerja sama internasional dijelaskan sebagai proses interaksi antara dua atau lebih pihak, di mana setiap entitas berusaha mencapai tujuan bersama atau

meningkatkan keuntungan bersama melalui koordinasi kebijakan, meskipun terdapat perbedaan aspirasi atau kepentingan nasional (Saeri, 2012). Definisi ini menekankan pentingnya interaksi dan koordinasi antarnegara atau entitas yang berdaulat dalam menghadapi isu-isu transnasional. Kerja sama semacam ini sering kali didasarkan pada keyakinan bahwa tantangan global atau regional tidak dapat diselesaikan sendirian. Oleh karena itu, aktivitas kolektif ini penting dalam merespons tantangan yang ada secara komprehensif dan terstruktur.

Hubungan kerja sama ini sering mengalami dinamika kompleks karena harus mempertimbangkan berbagai kepentingan multifaset dari setiap pihak yang terlibat. Menurut Heinl (2014), aspek kerja sama internasional juga harus memperhitungkan resistensi struktural dan institusional yang mungkin timbul dari dalam dan luar organisasi atau aliansi. Resistensi ini dapat berasal dari faktor-faktor seperti perbedaan budaya politik, sejarah diplomasi, hingga perbedaan tingkat pembangunan ekonomi yang mempengaruhi kapasitas dan kesiapan aktor dalam menerapkan kerangka kerja sama. Hal ini menunjukkan bahwa definisi kerja sama internasional tidak hanya tentang kerja sama formal, tetapi juga tentang strategi yang dilakukan untuk mengatasi hambatan sistemik dalam pelaksanaannya.

Kerangka kerja sama ini, jika diterapkan di tingkat regional, seperti dalam organisasi ASEAN, membutuhkan adaptasi terhadap tantangan lokal yang unik. Menurut Mohamed Mizan et al. (2019), definisi kerja

sama di tingkat regional, terutama dalam konteks keamanan siber, tidak semudah mengadopsi kerangka global; tetapi lebih tentang mengintegrasikan kapasitas lokal dan kebijakan nasional yang seimbang untuk mencapai efisiensi dan efektivitas yang diinginkan. Ini menunjukkan pentingnya pengembangan model kerja sama yang fleksibel dan kontekstual, yang dapat memenuhi kebutuhan khusus sambil menegaskan komitmen kolektif yang kuat dari setiap negara anggota.

Dengan memperhatikan kompleksitas dan dinamika dalam kerja sama internasional, dapat disimpulkan bahwa definisi tersebut secara intrinsik mengandung elemen adaptasi untuk menghadapi tantangan perubahan zaman dan perkembangan teknologi. Dalam realitas global yang semakin terhubung ini, aktor harus terus mengevaluasi strategi dan kebijakan mereka untuk memastikan hasil yang optimal. Evaluasi ini juga harus mempertimbangkan keberlanjutan dan harmoni regional untuk menjaga stabilitas yang pada akhirnya akan menguntungkan semua pihak yang terlibat dalam kerja sama internasional.

Landasan teori dalam kerja sama internasional berfungsi untuk memberikan kerangka konseptual dan analitis yang diperlukan dalam memahami dan menilai interaksi antar negara. Kerja sama internasional umumnya dianggap sebagai sarana untuk mencapai tujuan bersama yang tidak mungkin dicapai secara individual oleh negara-negara anggota (Saeri, 2012). Dalam konteks ASEAN, kerja sama internasional memainkan peran penting dalam mengatasi tantangan keamanan siber

yang berkembang pesat. Dengan semakin terhubungnya infrastruktur digital, negara-negara anggota ASEAN harus bekerja sama untuk menciptakan strategi keamanan siber yang efektif dan responsif (Heinl, 2014). Melalui kerangka kerja internasional, negara-negara dapat bertukar informasi, berbagi sumber daya, dan mengembangkan kebijakan bersama yang dirancang untuk melindungi kepentingan kolektif (Saeri, 2012).

Selain itu, fungsi kerja sama internasional juga terletak pada peningkatan kapasitas kolektif negara-negara dalam membangun ketahanan terhadap ancaman eksternal. Kerja sama ini memungkinkan negara-negara untuk saling mendukung dalam pengembangan kapasitas teknis dan kelembagaan yang diperlukan guna menghadapi tantangan bersama (Mohamed Mizan et al., 2019). Di ASEAN, kolaborasi internasional dalam keamanan siber membantu negara-negara anggota meningkatkan pemahaman dan keterampilan mereka dalam menangani insiden keamanan siber (Heinl, 2014). Ini juga mencakup pelatihan, pertukaran pengetahuan, dan pengembangan praktik terbaik yang disesuaikan dengan kebutuhan regional.

Kerja sama internasional juga berfungsi sebagai mekanisme koordinasi kebijakan di antara negara-negara yang berbeda namun memiliki kepentingan yang sama. Dalam kerangka ASEAN, ini menjadi sangat penting mengingat keberagaman politik dan ekonomi di antara negara anggotanya. Dengan adanya kerja sama, negara-negara tersebut dapat menyamakan persepsi dan pendekatan mereka terhadap masalah

keamanan siber, sehingga meminimalkan konflik kebijakan yang mungkin timbul (Saeri, 2012). Dengan demikian, kerja sama internasional menjadi alat yang esensial untuk membangun konsensus dan keselarasan kebijakan (Heinl, 2014).

Terakhir, kerja sama internasional memungkinkan pengembangan dan implementasi standar dan norma internasional yang dapat diadopsi secara luas. Fungsi ini sangat relevan di era digital saat ini, di mana ancaman siber tidak mengenal batas negara. Dengan terlibat dalam kerja sama internasional, negara-negara dapat bekerja sama dalam menetapkan standar keamanan yang kuat dan berlaku secara global (Mohamed Mizan et al., 2019). Ini tidak hanya meningkatkan keamanan jaringan dan sistem, tetapi juga memfasilitasi perdagangan dan komunikasi lintas batas yang lebih aman dan efisien. Oleh karena itu, kerja sama internasional memainkan peran yang sangat penting dalam menciptakan lingkungan siber yang aman dan berkelanjutan.

Pendalaman dalam ruang lingkup kerja sama internasional juga memperhatikan pentingnya hubungan antar-negara yang bersifat dinamis dan mungkin berubah seiring waktu. Aspek-aspek seperti keamanan regional, pertukaran teknologi, serta diplomasi publik menjadi integral dalam pengembangan kebijakan dan strategi yang efektif. Ruang lingkup ini menuntut adanya pemahaman mendalam tentang kerumitan hubungan internasional yang mana sering kali melibatkan aktor non-negara seperti organisasi internasional dan sektor swasta. Selain itu, jaringan lembaga

internasional dan mekanisme multilateral sering kali menjadi bagian dari kerangka kerja untuk mengkoordinasikan upaya kolektif. Melalui mekanisme ini, negara-negara dapat berbagi informasi, sumber daya, dan keahlian dalam menangani isu-isu yang melintasi batas wilayah nasional.

Lebih lanjut, ruang lingkup kerja sama internasional dan regional juga mensyaratkan adanya kesepahaman dan kesepakatan mengenai norma dan prinsip-prinsip dasar yang dijunjung bersama oleh negara-negara anggota. Pada kasus ASEAN, kerangka kerja ini sering kali menekankan konsensus dan non-intervensi sebagai prinsip utama dalam interaksinya. Hal ini berarti bahwa setiap kebijakan atau inisiatif yang diambil harus mempertimbangkan keberagaman pandangan dan kepentingan negara anggota, serta mendukung stabilitas dan perdamaian regional. Dalam hal ini, proses dialog dan konsultasi menjadi elemen penting yang harus dilakukan secara terus-menerus untuk memastikan kerja sama yang efektif dan berkelanjutan (Mohamed Mizan et al., 2019).

Di samping itu, pentingnya penilaian dan evaluasi berkala terhadap kebijakan dan strategi yang telah diimplementasikan juga menjadi bagian dari ruang lingkup kerja sama internasional. Evaluasi ini diperlukan untuk memantau efektivitas dan efisiensi dari berbagai program dan inisiatif yang telah dilaksanakan. Penilaian berkala memungkinkan negara-negara anggota untuk mengidentifikasi tantangan baru serta peluang untuk perbaikan, sementara juga memastikan bahwa tujuan bersama selalu menjadi prioritas. Dalam bidang keamanan siber, misalnya, penilaian

risiko dan respons yang cepat terhadap ancaman yang muncul mungkin diperlukan untuk melindungi infrastruktur kritis dan menjaga kepercayaan publik. Dengan demikian, kolaborasi berkelanjutan dan adaptabilisitas yang tinggi menjadi kunci keberhasilan dalam kerja sama internasional di era yang terus berubah ini.

Teori dasar yang berkaitan dengan sifat kerja sama internasional menunjukkan bagaimana elemen-elemen inti tersebut terbentuk dan berkembang (Saeri, 2012). Pada dasarnya, aspek utama dari kerja sama internasional adalah adanya tujuan bersama yang dicapai melalui kerja sama yang terkoordinasi antar negara. Tujuan tersebut sering kali memiliki cakupan yang luas dan melibatkan berbagai pihak di tingkat internasional untuk menyelesaikan masalah global yang rumit. Selain itu, kerja sama ini umumnya ditandai dengan keberadaan formalitas, seperti perjanjian atau kesepakatan yang terstruktur untuk memastikan keselarasan dalam pelaksanaan kebijakan dan strategi bersama. Formalitas ini sangat penting dalam menjaga stabilitas hubungan, mengingat adanya perbedaan kepentingan dan kedaulatan antar negara.

Sejalan dengan sifat tersebut, fleksibilitas dan adaptabilitas juga merupakan ciri penting dalam kerja sama internasional (Heinl, 2014). Fleksibilitas diperlukan untuk merespons perubahan dalam konteks geopolitik yang dinamis, yang dapat mempengaruhi kepentingan negara-negara yang terlibat. Selain itu, adaptabilitas memastikan bahwa berbagai pihak internasional, baik itu pemerintah, organisasi regional, maupun

organisasi non-pemerintah, dapat menyesuaikan peran mereka sesuai dengan situasi yang ada, sehingga kerja sama tetap relevan dan efektif dalam menghadapi perkembangan global. Adaptabilitas ini memungkinkan negara-negara untuk bekerja sama secara positif meskipun terdapat perbedaan budaya dan sistem politik.

Koordinasi menjadi faktor penting lainnya dalam mengoptimalkan kerja sama internasional (Mohamed Mizan et al., 2019). Melalui koordinasi yang efisien, para pelaku kerja sama dapat memastikan bahwa sumber daya yang tersedia dimanfaatkan secara efektif dan tidak terjadi tumpang tindih. Hal ini sangat penting terutama dalam menangani isu-isu lintas batas yang memerlukan respons kolektif, seperti keamanan siber di kawasan ASEAN. Bagi negara-negara anggota, koordinasi dapat diperkuat melalui pertukaran informasi yang relevan dan pembelajaran bersama dari praktik terbaik. Dengan demikian, koordinasi yang baik dapat meningkatkan kapasitas kolektif untuk menghadapi tantangan bersama.

Keberlanjutan menjadi sifat lain yang mencolok dalam kerja sama internasional. Keberlanjutan tersebut dicapai melalui pendekatan jangka panjang yang mempertimbangkan dampak dan manfaat dari kerja sama tersebut di masa depan (Heinl, 2014). Dalam konteks ini, perencanaan strategis menjadi elemen krusial yang harus diintegrasikan ke dalam proses pengambilan keputusan. Pendekatan keberlanjutan tidak hanya fokus pada pencapaian hasil dalam jangka pendek tetapi juga mempertimbangkan kelangsungan manfaat yang dirasakan oleh generasi

mendatang. Dengan pendekatan ini, kerja sama internasional dapat memberikan kontribusi yang signifikan terhadap stabilitas dan kesejahteraan global.

Indikator dalam kerja sama internasional memiliki peran penting dalam menilai efektivitas dan keberhasilan kerja sama antarnegara. Indikator ini dapat berupa parameter kualitatif maupun kuantitatif yang menunjukkan sejauh mana tujuan kerja sama tercapai. Pemilihan indikator yang tepat sangat penting untuk menentukan arah kebijakan dalam kerja sama internasional. Dalam konteks ASEAN, indikator sering mencakup aspek keamanan, ekonomi, dan politik yang saling terkait. Setiap indikator harus dianalisis secara menyeluruh agar dapat beradaptasi dengan dinamika hubungan internasional.

Penetapan indikator dalam kerja sama internasional juga penting untuk memastikan bahwa setiap negara anggota memiliki visi dan misi yang sama. Contohnya, dalam kerja sama keamanan siber ASEAN, indikator dapat termasuk peningkatan kapasitas negara anggota dalam menghadapi ancaman siber. Indikator keberhasilan lainnya meliputi peningkatan kolaborasi regional dan pengembangan kebijakan bersama. Dengan adanya indikator yang disepakati bersama, negara-negara anggota dapat mengevaluasi dan menyesuaikan strategi sesuai dengan perkembangan global.

Isu keamanan siber yang kompleks memerlukan indikator yang komprehensif dan adaptif. Indikator harus mencakup berbagai dimensi

kerja sama internasional, termasuk aspek teknis, kebijakan, dan tata kelola. Hal ini penting untuk membangun ketahanan siber di tingkat regional dan melindungi keamanan siber di ASEAN. Indikator juga berfungsi sebagai panduan untuk pengembangan kerja sama lebih lanjut, membantu dalam menghadapi tantangan dan peluang dalam kerja sama internasional.

Dengan evaluasi periodik, indikator dapat memastikan relevansi dan efektivitasnya dalam menjawab kebutuhan kontemporer. Dengan penggunaan indikator yang tepat dan konsisten, tujuan kerja sama internasional seperti dalam kerangka ASEAN dapat lebih mudah dicapai dan memberikan manfaat yang nyata bagi semua pihak terlibat.

## C. Penelitian Terdahulu

1. Nama Dan Judul:

- Nugraha (2023): Studi mengenai kerja sama dalam Strategi Kerja sama Keamanan Siber ASEAN dan dampaknya terhadap keamanan siber di wilayah tersebut, terutama di Indonesia.

- Laksmono dan Fauzi (2024): Penelitian mengenai diplomasi pertahanan melalui forum seperti Pertemuan Menteri Pertahanan ASEAN (ADMM) dalam mengatasi ancaman-ancaman termasuk terorisme.

2. Variabel:

- Variabel kerja sama regional dalam menghadapi ancaman siber yang semakin kompleks.

- Variabel diplomasi pertahanan dalam memfasilitasi koordinasi antar negara untuk mengatasi ancaman-ancaman termasuk terorisme.

3. Persamaan Penelitian:

- Keduanya menekankan pentingnya kerja sama regional dalam menghadapi ancaman keamanan non-tradisional.

- Fokus pada peran kolektif negara-negara ASEAN dalam menangani kejahatan siber.

4. Perbedaan Penelitian:

- Nugraha (2023) lebih menyoroti dampak strategi keamanan siber terhadap stabilitas keamanan di wilayah tersebut.

- Laksmono dan Fauzi (2024) lebih menekankan bagaimana forum seperti ADMM dapat berperan sebagai platform efektif dalam kebijakan pertahanan terhadap ancaman lintas negara.