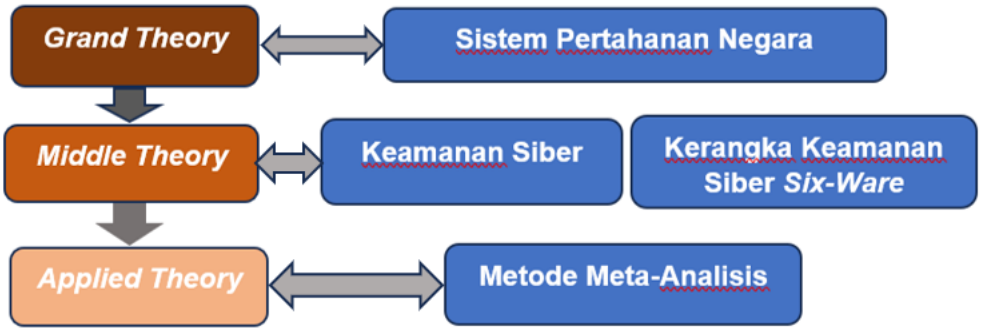
BAB 2
TINJAUAN PUSTAKA

2.1 Landasan Teori

Dalam penelitian ini akan menyajikan kerangka teoritis yang menjadi dasar untuk memahami dan menganalisis topik penelitian ini. Kerangka teoritis ini akan memberikan pemahaman mendalam tentang konsep-konsep kunci, kerangka kerja, dan prinsip-prinsip yang relevan terkait dengan subjek penelitian. Dengan menggunakan kerangka teoritis ini, bertujuan untuk memperluas pemahaman tentang topik penelitian, memberikan konteks yang diperlukan, dan membangun dasar yang kokoh untuk penelitian secara keseluruhan. Oleh karena itu, dalam bab ini, Penulis akan menjelaskan dengan lebih detail kerangka teoritis yang digunakan sebagai dasar intelektual untuk penelitian ini.



Gambar 2. 1 Tingkatan Teori yang Digunakan
Sumber: Penulis (2023)

2.1.1. Sistem Pertahanan Negara

Sistem pertahanan negara Indonesia yang bersifat semesta melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainnya, serta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut. Konsep ini mencakup upaya mempertahankan kedaulatan negara, keutuhan wilayah NKRI, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara. Dalam konteks keamanan siber dan pertahanan siber, peraturan per undang-undangan

Indonesia juga memiliki peran penting dalam mendukung sistem pertahanan negara (Manihuruk, 2020) (Azikin et al., 2020)

Partisipasi dan keterlibatan semua elemen masyarakat, termasuk warga negara, sangat penting dalam menjaga integritas dan keamanan negara (Mardhani et al., 2002). Kebijakan Keamanan dan Pertahanan siber yang diselenggarakan oleh Negara bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi penting bagi negara dan keamanan nasional, serta menjaga Sistem Elektronik strategis atau kritis (Coyne & Hall, 2019). Undang-undang No. 3 tahun 2002 tentang Pertahanan Negara menetapkan sistem pertahanan universal yang melibatkan semua warga negara, wilayah, dan sumber daya nasional (GÜLER & KİŞMAN, 2020). Ini menunjukkan pentingnya partisipasi semua elemen masyarakat, termasuk warga negara, dalam memastikan integritas dan keamanan negara (Štitilis et al., 2016). Kebijakan Keamanan dan Pertahanan siber dirancang untuk melindungi informasi penting dan memastikan kelangsungan layanan publik dan negara (Coyne, 2015).

Cybersecurity dan *cyberdefense* dapat diatur di tingkat individu, kolektif, atau nasional. Setiap ruang lingkup dapat bervariasi dalam hal pendekatan dan strateginya. Dalam kasus Indonesia, pemerintah telah menerapkan peraturan khusus, seperti Undang-Undang Nomor 11 Tahun 2008, untuk memperkuat hukum siber dan melindungi negara dari ancaman siber (Cîrdei & Bojor, 2020). Tujuannya adalah untuk membangun Sistem Elektronik yang solid, andal, dan aman yang selaras dengan prinsip pertahanan nasional, yang menekankan sifat universal pertahanan (Manihuruk, 2020). Membangun kemampuan, melawan ancaman, dan memastikan keamanan negara dan bangsa adalah komponen penting dari pertahanan nasional dalam domain siber (Giles et al., 2015). Dengan menerapkan peraturan yang ketat dan mengorganisir upaya pertahanan siber, Indonesia bertujuan untuk

membangun keamanan global dan melindungi diri dari kejahatan siber (Tehan, 2016).

Cybersecurity dan *cyberdefense* sangat penting untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi penting dan melindungi sistem elektronik penting. Peraturan Indonesia, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, mendukung pentingnya keamanan siber dalam mendukung pertahanan negara dan kedaulatan negara (Sandjojo et al., 2020). Perkembangan teknologi informasi di dunia maya telah menyebabkan meningkatnya kerentanan terhadap ancaman dan serangan terhadap lalu lintas data dan informasi, sehingga perlu untuk memperkuat infrastruktur dan institusi siber Indonesia (Setiyawan, 2019). Meningkatnya penggunaan dan ketergantungan pada teknologi informasi dan komunikasi di Indonesia telah membuat kerentanan keamanan dan pertahanan di dunia maya menjadi isu terpisah (Aulianisa & Indirwan, 2020). Membangun infrastruktur vital nasional dan memberlakukan peraturan tentang keamanan dan ketahanan siber sangat mendesak untuk melindungi kedaulatan negara dan kepentingan nasional (Alhayani et al., 2021) (Aswandi et al., 2020). Kehadiran *cybercrime* menimbulkan ancaman bagi kehidupan manusia dan menyoroti perlunya sistem seperti Indonesian Data Protection System (IDPS) untuk mengelola data dan informasi pribadi dengan aman.

2.1.2. Pertahanan dan Keamanan Siber

Keamanan siber terkait pertahanan negara adalah suatu upaya untuk melindungi sistem informasi, jaringan komputer, dan data dari akses yang tidak sah, penggunaan yang tidak sah, pengungkapan yang tidak sah, penghancuran yang tidak sah, dan gangguan yang tidak sah. Keamanan siber juga meliputi perlindungan terhadap serangan siber yang dapat merusak infrastruktur kritis, seperti sistem kelistrikan, sistem

air, dan sistem transportasi. Menurut Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 pertahanan siber mengacu pada langkah-langkah dan strategi yang diterapkan untuk melindungi sistem komputer, jaringan, dan data dari ancaman dan serangan siber. Ini melibatkan penggunaan berbagai teknologi, kebijakan, dan praktik untuk mendeteksi, mencegah, dan menanggapi insiden siber dan memastikan keamanan dan ketahanan sistem informasi. Pertahanan siber bertujuan untuk melindungi terhadap akses tidak sah, pelanggaran data, infeksi malware, dan aktivitas jahat lainnya yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan aset digital. Ini mencakup kegiatan seperti manajemen kerentanan, respons insiden, pemantauan jaringan, kontrol akses, dan pelatihan kesadaran keamanan. Pertahanan siber adalah komponen penting dari keamanan siber dan sangat penting bagi organisasi dan pemerintah untuk melindungi infrastruktur penting dan informasi sensitif organisasi. Dalam dunia digital, pertahanan dan keamanan siber sangat penting karena semakin banyaknya data yang disimpan secara digital dan semakin banyaknya aktivitas yang dilakukan secara online.

Pertahanan dan keamanan siber juga penting dalam menjaga keamanan nasional, karena serangan siber dapat membahayakan infrastruktur kritis dan informasi rahasia negara. Selain itu, keamanan siber juga penting dalam menjaga privasi dan keamanan data pribadi pengguna internet. Ancaman siber yang meluas dan serius dapat menyebabkan kerugian finansial, kerugian reputasi, dan bahkan kerugian nyawa. Serangan siber dapat merusak infrastruktur kritis, seperti sistem kelistrikan, sistem air, dan sistem transportasi, yang dapat mengakibatkan kerugian finansial dan kerugian nyawa. Selain itu, serangan siber juga dapat merusak reputasi perusahaan atau negara, karena dapat mengakibatkan kebocoran data rahasia atau pencurian data pribadi pengguna internet.

Untuk menghadapi ancaman siber yang semakin kompleks dan meluas, diperlukan langkah-langkah keamanan siber yang kuat. Beberapa langkah yang dapat dilakukan antara lain:

1) Pendidikan dan Pelatihan: Pendidikan dan pelatihan mengenai keamanan siber dapat membantu meningkatkan kesadaran dan keterampilan pengguna internet dalam menghadapi ancaman siber (Alhayani et al., 2021).
2) Penggunaan Teknologi Keamanan: Penggunaan teknologi keamanan, seperti firewall, antivirus, dan enkripsi, dapat membantu melindungi sistem informasi dan data dari serangan siber (Rathod & Hämäläinen, 2020).
3) Kerjasama Internasional: Kerjasama internasional dapat membantu menghadapi ancaman siber yang melintasi batas negara (Srinivas et al., 2019).
4) Pengembangan Hukum: Pengembangan hukum yang berkaitan dengan keamanan siber dapat membantu menegakkan hukum terhadap pelaku kejahatan siber (Chan et al., 2018).
5) Dalam menjaga keamanan jaringan komputer, terdapat beberapa prinsip keamanan jaringan yang harus diterapkan, yaitu *confidentiality* (kerahasiaan), *authentication* (autentikasi), *integrity* (integritas), *availability* (ketersediaan data), dan *access control* (kontrol akses) (Kosseff, 2018).

Dalam rangka mendukung pertahanan negara, keamanan siber menjadi hal yang sangat penting untuk diperhatikan. Ancaman siber yang semakin kompleks dan meluas dapat membahayakan infrastruktur kritis dan informasi rahasia negara. Oleh karena itu, diperlukan langkah-langkah keamanan siber yang kuat untuk menghadapi ancaman siber tersebut.

Keamanan siber memiliki peran penting dalam dunia digital. Dalam era digital saat ini, keamanan siber menjadi krusial karena semakin banyaknya data yang disimpan secara digital dan semakin

luasnya penggunaan teknologi. Keamanan siber berperan dalam melindungi data dan informasi dari akses yang tidak sah dan penggunaan yang tidak sah (Dutta et al., 2022). Selain itu, keamanan siber juga berperan dalam mencegah serangan siber yang dapat merusak sistem dan infrastruktur. Serangan siber dapat menyebabkan kerusakan serius, termasuk kehilangan data penting, gangguan layanan, dan hilangnya kepercayaan publik (Tomsu, 2021). Keamanan siber juga penting dalam menjaga kepercayaan publik terhadap sistem dan layanan digital. Dengan adanya keamanan siber yang baik, pengguna dapat merasa lebih aman dan percaya dalam menggunakan layanan digital (Salih et al., 2021).

Langkah-langkah keamanan siber yang kuat diperlukan untuk melindungi infrastruktur penting, seperti sistem kelistrikan, sistem air, dan sistem transportasi, dari serangan siber yang berpotensi merusak (S. Singh & Phadke, 2021). Serangan siber terhadap infrastruktur kritis dapat menyebabkan gangguan serius dan membahayakan kehidupan manusia (Cali et al., 2021). Ancaman siber yang semakin kompleks dan meluas menimbulkan risiko bagi infrastruktur penting dan informasi rahasia negara (M. Singh, 2021). Tindakan keamanan siber yang kuat diperlukan untuk mengatasi ancaman ini (West & Zentner, 2019). Di Indonesia, keamanan siber diatur oleh undang-undang seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penerapan Sistem dan Transaksi Elektronik (Bajaj & Akhilesh, 2019). Undang-undang ini bertujuan untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi yang penting bagi negara dan keamanan nasional, serta kelangsungan pelayanan publik. Rancangan Undang-Undang tentang Keamanan Siber dan Ketahanan di Indonesia mencakup pasal-pasal tentang prinsip-prinsip keamanan siber, kebijakan keamanan siber, serta tugas dan otoritas Badan siber dan Sandi Negara (BSSN).

Peraturan di Indonesia mendukung pentingnya keamanan siber dalam mendukung pertahanan negara dan menjaga sistem elektronik kritis.

Keamanan siber menjadi hal yang sangat penting dalam mendukung pertahanan negara. Ancaman siber yang semakin kompleks dan meluas dapat membahayakan infrastruktur kritis dan informasi rahasia negara. Oleh karena itu, diperlukan langkah-langkah keamanan siber yang kuat untuk menghadapi ancaman siber tersebut. Beberapa praktik pengaturan keamanan siber di beberapa negara mendukungnya mempunyai arti dan peranan yang penting dalam (Alhayani et al., 2021). Selain itu, kerangka kerja untuk meningkatkan keamanan siber infrastruktur kritis juga menjadi hal yang penting untuk diperhatikan. Kerangka kerja ini dapat membantu organisasi dalam mengatasi risiko-risiko keamanan siber. Selain itu, pendidikan dan pelatihan mengenai keamanan siber dapat membantu meningkatkan kesadaran dan keterampilan pengguna internet dalam menghadapi ancaman siber (Bajaj & Akhilesh, 2019). Penggunaan teknologi keamanan, seperti *firewall*, antivirus, dan enkripsi, juga dapat membantu melindungi sistem informasi dan data dari serangan siber (Kosseff, 2018). Pembentukan regulasi yang berkaitan dengan keamanan siber dapat membantu menegakkan hukum terhadap pelaku kejahatan siber. Pembangunan CSIRT (*Computer Security Incident Response Team*) juga dapat membantu mengidentifikasi dan menangani serangan siber dengan cepat dan efektif (Carneiro, 2016). Oleh karena itu, untuk mendukung pertahanan negara, keamanan siber harus menjadi prioritas dan diperlukan langkah-langkah keamanan siber yang kuat.

2.1.3. Kerangka Keamanan Siber *Six-Ware* (SWCSF)

Di era digital yang semakin berkembang, tantangan keamanan siber telah menjadi salah satu isu kritis bagi organisasi, entitas, dan negara. Dalam lingkungan yang dipenuhi dengan teknologi canggih, konektivitas global, dan ancaman yang semakin kompleks, perlindungan

terhadap data, informasi, dan infrastruktur menjadi lebih penting dari sebelumnya. Keamanan siber tidak lagi dapat dianggap sebagai masalah teknis semata, melainkan sebagai landasan strategis yang melibatkan dimensi manusia, teknologi, dan pengelolaan (Tomsu, 2021). Dalam konteks inilah Konsep Kerangka Keamanan SWCSF muncul sebagai panduan esensial dalam menghadapi perubahan lanskap keamanan siber yang dinamis.

Kerangka Keamanan SWCSF merupakan konsep yang sangat penting dalam upaya meningkatkan keamanan siber suatu entitas atau organisasi. Konsep ini memiliki tujuan mendasar untuk mengatasi tantangan dan ancaman yang semakin berkembang dalam dunia digital, serta untuk melindungi integritas, kerahasiaan, dan ketersediaan data dan informasi. SWCSF mencakup enam dimensi utama yang dikenal sebagai "*ware*" yang saling terkait dan saling mempengaruhi untuk membentuk landasan keamanan yang kokoh (M. Susiana et al., 2022)(Hutomo et al., 2021)(Meylia Susiana Dewi Putri et al., 2023).

1) *Brainware* (Faktor Manusia): Dimensi ini mengakui peran krusial yang dimainkan oleh manusia dalam ekosistem keamanan siber. Meskipun teknologi semakin canggih, manusia tetap menjadi faktor terpenting. Kecermatan, keterampilan, dan perilaku pengguna dapat memiliki dampak besar pada kerentanan atau ketangguhan suatu sistem terhadap serangan siber. Pentingnya kesadaran keamanan dan pelatihan bagi setiap anggota organisasi tidak dapat diabaikan. Melalui edukasi yang baik, orang dapat menjadi pertahanan pertama dalam menghadapi upaya peretasan (Hutomo et al., 2021).
2) *Hardware* (Perangkat Keras): Perangkat keras merupakan komponen fisik dari sistem teknologi informasi. Di sinilah data diproses, disimpan, dan dikirim. Pengamanan perangkat keras adalah kunci dalam menghadapi ancaman seperti manipulasi perangkat keras, serangan fisik, dan perangkat keras yang telah diretas. Menyadari pentingnya peran perangkat keras dalam ekosistem siber, organisasi

harus memiliki strategi yang kuat untuk mengamankan perangkat keras, termasuk penerapan tindakan fisik dan kontrol akses yang ketat (Hutomo et al., 2021).

3) *Software* (Perangkat Lunak): Perangkat lunak mencakup semua aplikasi dan program yang digunakan dalam operasional sehari-hari organisasi. Karena perangkat lunak memiliki kerentanan yang dapat dimanfaatkan oleh peretas, memastikan bahwa perangkat lunak yang digunakan aman sangatlah penting. Ini melibatkan mengamankan aplikasi, menggunakan patch terbaru, dan memastikan bahwa perangkat lunak yang digunakan sesuai dengan standar keamanan (Hutomo et al., 2021) (Putri et al., 2023).
4) *Infrastructureware* (Infrastruktur Jaringan): Infrastruktur jaringan adalah fondasi dari operasi digital organisasi. Merupakan kewajiban untuk membangun dan menjaga lingkungan jaringan yang aman. Ini melibatkan pemantauan aktif terhadap ancaman, menerapkan kontrol akses yang ketat, dan mengembangkan rencana darurat untuk menghadapi insiden keamanan. Dengan semakin banyaknya perangkat yang terhubung melalui internet (Internet of Things), penting untuk memastikan bahwa jaringan dan perangkat terlindungi dengan baik (Hutomo et al., 2021).
5) *Firmware* (Perangkat Lunak Khusus): *Firmware* adalah perangkat lunak yang tertanam dalam perangkat keras dan bertanggung jawab atas operasionalitas dasar perangkat tersebut. Memastikan keamanan firmware adalah hal yang krusial untuk mencegah eksploitasi yang dapat mengancam keseluruhan sistem. Pemantauan, pembaruan, dan pengujian firmware secara berkala adalah langkah penting dalam memastikan integritas system (Gultom et al., 2018).
6) *Budgetware* (Anggaran Keamanan): Tidak dapat diabaikan bahwa investasi finansial dalam keamanan siber adalah kunci untuk kesuksesan keamanan organisasi. Alokasi anggaran yang memadai

untuk peralatan, pelatihan, sertifikasi, dan tindakan keamanan lainnya adalah langkah penting dalam memastikan keberhasilan strategi keamanan siber. Tanpa dukungan finansial yang memadai, upaya keamanan mungkin tidak efektif (Hutomo et al., 2021) (Gultom et al., 2018).

Dengan memahami dan menerapkan keseluruhan konsep SWCSF, organisasi dapat menghadapi tantangan keamanan siber dengan lebih baik. Pendekatan yang holistik ini mengakui bahwa keamanan siber bukanlah tanggung jawab tunggal, tetapi adalah hasil kerjasama antara manusia, perangkat keras, perangkat lunak, infrastruktur jaringan, perangkat lunak khusus, dan dukungan finansial yang memadai (Gultom et al., 2018). Melalui implementasi konsep SWCSF, organisasi dapat menciptakan ekosistem yang aman, tangguh, dan siap menghadapi ancaman siber yang terus berkembang.

Dengan mengadopsi SWCSF, organisasi dan negara dapat membangun fondasi yang kokoh dalam menghadapi perubahan keamanan siber yang cepat dan kompleks. Ini bukanlah sekadar metode, tetapi sebuah filosofi yang mengakui bahwa keamanan siber melibatkan semua pihak yang terlibat. SWCSF mendorong pengintegrasian pengetahuan, tindakan, dan alokasi sumber daya untuk menciptakan ekosistem yang aman, tangguh, dan siap menghadapi tantangan siber di masa depan. Dalam konteks ini, memahami lebih dalam tentang enam dimensi utama dari SWCSF dan bagaimana interaksi untuk menciptakan keamanan siber yang holistik dan efektif.

2.1.4. Definisi dan Ruang Lingkup Meta-Analisis

Pada 1904, Karl Pearson memperkenalkan konsep meta-analisis sebagai alat penelitian terutama untuk studi-studi dalam ranah kesehatan dan medis. Seiring waktu, metode ini telah dikembangkan dan diterapkan dalam beragam bidang dan topik penelitian. Sejak tahun 1970-an, Gene Glass, Frank L. Schmidt, dan John E. Hunter mulai memanfaatkan meta-

analisis dalam konteks pendidikan. Gene Glass secara khusus pada tahun 1976 mengemukakan pentingnya penelitian meta-analisis dalam dunia pendidikan, terutama mengingat banyaknya hasil penelitian terkait pengukuran keamanan siber yang tidak dieksplorasi lebih lanjut. Saat itu, pemahaman tentang meta-analisis dalam pertahanan siber masih terbatas.

Meta-analisis adalah prosedur statistik yang mengintegrasikan hasil beberapa penelitian independen yang dianggap "dapat digabungkan (Egger et al., 1997)." Meta-analisis yang dilakukan dengan baik memungkinkan penilaian bukti yang lebih obyektif dibandingkan tinjauan narasi tradisional, memberikan perkiraan efek pengobatan yang lebih tepat, dan dapat menjelaskan heterogenitas antara hasil penelitian individual. Sebaliknya, meta-analisis yang dilakukan dengan buruk mungkin menjadi bias karena pengecualian penelitian yang relevan atau dimasukkannya penelitian yang tidak memadai. Analisis yang menyesatkan umumnya dapat dihindari jika beberapa prinsip-prinsip penelitian mendasar diperhatikan.

Meta-analisis harus dipandang sebagai studi observasional terhadap bukti. Langkah-langkah yang dilakukan serupa dengan penelitian lainnya: perumusan masalah yang ingin diatasi, pengumpulan dan analisis data, serta pelaporan hasilnya. Peneliti harus menulis terlebih dahulu protokol penelitian terperinci yang dengan jelas menyatakan tujuan, hipotesis yang akan diuji, subkelompok yang diminati, dan metode serta kriteria yang diusulkan untuk mengidentifikasi dan memilih penelitian yang relevan serta mengekstraksi dan menganalisis informasi (Borenstein et al., 2021). Terkait dengan kriteria untuk memasukkan dan mengeluarkan data, kriteria kelayakan harus ditentukan agar data dapat dimasukkan. Kriteria berkaitan dengan kualitas riset dan kombinasi variabel, target, dan hasil. Menurut (Glass & Smith, 1979; GLASS, 1976), meta-analisis memiliki beberapa ciri khas, seperti:

1) Mencakup tinjauan literatur,
2) Menggunakan ringkasan hasil statistik daripada data mentah,
3) Melibatkan sejumlah besar studi atau penelitian,
4) Berfokus pada *effect size* intervensi daripada hanya signifikansi statistik
5) Memperhitungkan hubungan antara komponen penelitian dan hasilnya.

Meta-analisis saat ini paling sering digunakan dalam uji klinis, yang memang memiliki desain yang lebih terstruktur dan menyediakan bukti kausal yang lebih kuat. Namun, meta-analisis juga bisa diterapkan pada berbagai jenis studi observasional untuk menghasilkan kesimpulan yang didasarkan pada gabungan hasil penelitian (Schmid et al., 2020).

Penelitian meta-analisis, juga dikenal sebagai penelitian meta atau penelitian meta, melibatkan sintesis beberapa studi pada topik atau tema tertentu untuk mengekstrak temuan inti dan memberikan ringkasan hasil penelitian. Metode ini memanfaatkan sumber-sumber literatur seperti buku dan jurnal sebagai dasar pengumpulan dan analisis data. Ini bisa bersifat kuantitatif, yang melibatkan analisis statistik data dari penelitian sebelumnya. Meta-analisis telah dilakukan di berbagai bidang, termasuk penelitian organisasi dan manajemen (Fendt, 2023), studi tentang senyawa asal botani sebagai insektisida (Collares et al., 2023), penelitian kesehatan klinis (Fundaun et al., 2022), dan tinjauan sistematis dan meta-analisis dalam berbagai disiplin ilmu (Cannarella et al., 2022). Meta-analisis ini bertujuan untuk menghasilkan pengetahuan tingkat tinggi, mengidentifikasi tren dan bias, dan memberikan pedoman berbasis bukti untuk penelitian dan pengambilan keputusan di masa depan.

Dalam melakukan penelitian meta-analisis, ada beberapa langkah yang harus diikuti:

1) Langkah pertama adalah perumusan masalah, di mana Penulis memilih penelitian berdasarkan kriteria tertentu seperti

pengobatan, kontrol, dan prosedur percobaan, serta ukuran serupa dari hasil studi (Gasparini et al., 2021).

2) Langkah kedua adalah pengumpulan dan evaluasi data, yang melibatkan penggalian data yang relevan dari studi yang memenuhi syarat (Shah et al., 2020).
3) Langkah ketiga adalah analisis dan interpretasi data, di mana *effect size* dihitung dan model meta-analitik dibuat untuk menilai kekuatan efek dan menyelidiki kemungkinan moderator (Schmid et al., 2020).
4) Langkah terakhir adalah pelaporan hasil penelitian, di mana temuan didokumentasikan dan disebarluaskan kepada pemangku kepentingan yang berbeda (Forero et al., 2019).

Langkah-langkah ini memastikan pendekatan yang sistematis dan ketat untuk melakukan meta-analisis dan mensintesis bukti yang tersedia. Perumusan masalah adalah langkah awal dan sangat krusial. Penulis harus memilih penelitian yang akan digunakan berdasarkan kriteria tertentu seperti prosedur perlakuan, kontrol, dan percobaan, serta ukuran hasil penelitian yang serupa. Data yang dikumpulkan untuk meta-analisis terdiri dari isi penelitian dan indeks ekstraksi kuantitatif dari karakteristik penelitian dan besarnya efek (Rasouli et al., 2018).

Meta-analisis adalah teknik statistik yang menggabungkan *effect size* dari beberapa penelitian untuk memberikan perkiraan efek keseluruhan yang lebih andal. *Effect size* biasanya dihitung menggunakan perbedaan rata-rata antara perlakuan dan kelompok kontrol. Ada metode yang berbeda untuk menghitung *effect size* dan interval kepercayaan terkait, korelasi *effect size*, nilai-p, dan ukuran heterogenitas dan bias publikasi. Interpretasi *effect size* sebagai kecil, sedang, atau besar telah dipandu oleh tolok ukur konvensional atau perbandingan dengan penelitian sebelumnya. Namun, temuan terbaru menunjukkan bahwa bias seperti bias publikasi dan praktik penelitian yang dipertanyakan telah menyebabkan inflasi dalam efek yang dipublikasikan, sehingga sulit untuk

membandingkan efek aktual dengan efek populasi nyata. Diperlukan lebih banyak studi pra-registrasi untuk mendapatkan gambaran yang dapat diandalkan tentang efek populasi (Erah et al., 2021; Schäfer & Schwarz, 2019). Bias publikasi, di mana hanya hasil signifikan yang dilaporkan, dapat menyebabkan perkiraan *effect size* yang berlebihan. Metode telah dikembangkan untuk memperkirakan *effect size* sebenarnya dan prevalensi bias publikasi menggunakan statistik tes yang diterbitkan (Ulrich et al., 2018). Meta-analisis sering mengasumsikan independensi di antara *effect size*, tetapi ada situasi di mana *effect size* dapat bergantung, seperti ketika beberapa *effect size* dilaporkan pada konstruksi yang sama atau ketika dilaporkan oleh peserta dari kelompok budaya yang sama (Cheung, 2014). Praktik pelaporan indikator *effect size* tanpa perkiraan interval memiliki keterbatasan, dan penggunaan ukuran standar dalam psikologi dan bidang terkait dapat membatasi penggunaan *effect size* (Lecoutre & Poitevineau, 2014).

2.1.5. Model Statistik dalam Konteks Meta-Analisis

Pengolahan dan interpretasi data melalui metode statistik merupakan komponen inti dalam penelitian meta-analisis. Oleh karena itu, ada berbagai model statistik yang digunakan dalam meta-analisis untuk mengekstrak temuan dan interpretasi yang valid. Model statistik yang digunakan dalam meta-analisis dapat dikategorikan menjadi dua jenis: model yang hanya berfokus pada *effect size* dari berbagai studi, dan model yang mencakup informasi dan analisis tambahan bersama dengan *effect size*. Model statistik yang hanya fokus pada *effect size* biasanya dibagi menjadi dua jenis, yaitu model efek tetap (*fixed effect model*) dan model efek acak (*random effect model*). Tujuan penelitian Sedat Demir adalah untuk membandingkan kinerja Model Efek Tetap (FEM) dan Model Efek Acak (REM) dalam studi meta-analisis. Mereka menemukan bahwa REM lebih menguntungkan untuk kumpulan data dengan *outlier*, sementara FEM dan REM menghasilkan hasil yang serupa untuk kumpulan data tanpa

outlier (Demir, 2022). (Van Den Heuvel et al., 2022) Membahas pentingnya menggunakan beberapa model simulasi data agregat untuk mengevaluasi kinerja metode meta-analisis. Mereka merekomendasikan untuk membuat model data peserta individu eksplisit untuk menentukan pilihan distribusi dari statistik data agregat yang digunakan dalam simulasi. (Arian & Soleimani, 2020) Menjelaskan bahwa Penulis menggunakan berbagai metode statistik, seperti integrasi logaritmik dan skor-T, untuk menggabungkan hasil studi dalam meta-analisis. Namun, metode ini mungkin tidak secara akurat mewakili kekuatan atau intensitas hubungan. (Rose et al., 2020) Mengusulkan model multivariat baru untuk meta-analisis yang mendekati matriks varians-kovarians menggunakan proyeksi acak. Model ini mengurangi jumlah parameter yang perlu diperkirakan, membuat estimasi lebih mudah dilacak

Model efek tetap bertujuan untuk mengkalkulasi bobot rata-rata dari berbagai studi yang termasuk dalam analisis meta-analisis. Dari perspektif statistik, model ini mengasumsikan bahwa semua studi atau penelitian dalam meta-analisis mengacu pada populasi yang sama dan mengevaluasi variabel yang identik. Oleh karena itu, studi dengan jumlah sampel yang besar biasanya akan memberikan bobot yang lebih signifikan dalam hasil akhir meta-analisis. Dalam konteks di mana sebagian besar studi dalam meta-analisis berskala besar, dampak dari studi berskala kecil pada hasil dan interpretasi akhir akan menjadi minimal (Pham et al., 2023).

Di sisi lain, model efek acak digunakan ketika ada variasi atau heterogenitas antar penelitian yang diikutsertakan dalam meta-analisis. Model ini menghasilkan bobot rata-rata dari *effect size* dari kelompok penelitian, tanpa mempertimbangkan bobot individual dari masing-masing studi. Secara teoretis, model efek acak diperoleh melalui dua langkah: pertama, melakukan inversi varian dari bobot studi yang ada, dan kedua, menghilangkan bobot yang telah diinversi.

Selain itu, ada juga model statistik yang memasukkan informasi dan analisis tambahan, seperti model efek kualitas (*quality effect model*)

(Kanters, 2022). Model ini merupakan metode statistik yang dirancang untuk menyesuaikan heterogenitas antar studi dalam meta-analisis dengan mempertimbangkan varian dan kualitas dari masing-masing studi. Dalam model ini, bukti empiris atau metodologis juga dianggap dalam perhitungan, bukan hanya berdasarkan angka statistik semata. Varian bias dihitung berdasarkan kualitas data yang digunakan dalam analisis (Cleophas & Zwinderman, 2017)**.**

2.2 Hasil Penelitian Terdahulu

Di segmen ini, hasil dari studi-studi sebelumnya yang berhubungan dengan tema penelitian akan diuraikan. Melalui survei literatur yang mendalam, Penulis telah mengkompilasi dan memeriksa berbagai penelitian yang sebelumnya telah dijalankan dan yang memiliki keterkaitan dengan topik atau aspek-aspek yang serupa dengan fokus penelitian ini. Keberadaan hasil dari penelitian-penelitian ini memberikan perspektif dan temuan yang berarti, yang bisa berfungsi untuk memperkaya pemahaman terhadap subjek yang sedang diteliti, menemukan celah-celah dalam pengetahuan yang ada, serta membentuk rumusan penelitian yang sesuai. Di dalam bab ini, Penulis akan menggambarkan dengan detail hasil-hasil dari penelitian-penelitian tersebut, membandingkan berbagai temuan yang telah ada, dan menilai kelebihan serta kekurangan dari tiap-tiap studi. Dengan mempertimbangkan hasil-hasil dari penelitian-penelitian ini, harapannya adalah untuk memunculkan kontribusi yang inovatif dan unik dalam penelitian ini.

Dari 10 penlitian terdahulu yang relevan, penelitian nomor 1 sampai 9 adalah yang paling relevan dengan penelitian ini. Dimana penelitian tersebut berkaitan dengan fenomena masalah yang relative sama yaitu tentang pengembangan kerangka kerja SWCSF dalam pertahan siber untuk mendukung pertahanan neraga, sementara perbedaannya yaitu terkait metode penelitian, parameter dan variable yang digunakan, tujuan penelitian. Kemudian untuk penelitian nomor 9 dan 10 memiliki kesamaan

dalam metode penelitian yaitu meta analisis dan memiliki perbedan di parameter dan variable yang digunakan, tujuan penelitian, objek penelitian, dan fenomena masalah. Terkait hal tersebut maka novelty dari penelitian ini adalah evaluasi komprehensif efektivitas SWCDF, identifikasi faktor-faktor yang Mempengaruhi efektivitas SWCDF, pembandingan Metode Evaluasi yaitu dengan metode meta analisis di dalam pemngembangan kerangka kerja SWCDF untuk pertahanan siber. Ringkasan penelitian terdahulu terdapat pada **Tabel 2.1.**

Tabel 2. 1 Hasil Penelitian Terdahulu

No.	Nama Penulis dan Tahun Penelitian	Judul Penelitian	Hasil dan Pokok Penelitian	Perbedaan
1.	Rudy Agus Gemilang Gultom, Ahmad Farid Wajdi (2022)	*Development of Six Ware Cyber Defense Framework (SWCDF) Design as a Standardization of Computer Network Protection State Defense Information System*	Subjek Penelitian: 1) Penelitian ini berfokus pada desain sistem pertahanan siber yang efektif untuk melindungi infrastruktur penting dan sistem informasi pertahanan negara (Sisinfohanneg) dari Kementerian Pertahanan dari serangan siber. Ini juga bertujuan untuk mempersiapkan kemampuan perang siber. Hasil Penelitian: 1) Penelitian ini mengusulkan konsep pengukuran yang disebut indeks ICSW, yang merumuskan *Six Ware Cyber Defense Framework*. Kerangka kerja ini terdiri dari enam faktor: *Brainware, Hardware, Software,*	Parameter dan variable yang digunakan, tujuan penelitian, metode penelitian.

			Infrastructureware, Firmware, dan Budgetware. Ketersediaan rumus pengukuran meningkatkan implementasi kerangka kerja. 2) Studi ini juga bertujuan untuk mengembangkan sistem aplikasi untuk mengidentifikasi kerentanan sistem pertahanan siber dengan cepat dan akurat, yang dapat berfungsi sebagai referensi untuk membangun sistem pertahanan siber yang kuat di lembaga lain. 3) Penelitian ini menekankan meningkatnya kompleksitas ancaman pertahanan dunia maya dan kebutuhan untuk beradaptasi dengan kondisi masa depan. Ini menyoroti urgensi memperkuat pertahanan dunia maya, membentuk Tim Tanggap Darurat Komputer (CERT), dan melindungi	

			infrastruktur penting dan sistem informasi pertahanan nasional dari serangan siber.	
2.	Rudy Agus Gemilang Gultom, Asep Adang Supriyadi, Tatan Kustana (2018)	*Strengthening Asean Cyber Cooperation in Countering Cyber Terrorist Groups Activities on the Internet by Impelmenting the Six-Ware Cyber Security*	Subjek Penelitian: 1) Subjek penelitian adalah perlunya standar ASEAN *Cyber Security Framework* untuk melawan aktivitas terorisme siber di internet. 2) Penelitian ini menekankan dampak negatif pemanfaatan internet oleh kelompok ekstremis, radikal, dan teroris, yang menggunakannya untuk kegiatan seperti perekrutan anggota, propaganda, penggalangan dana, dan serangan siber. 3) Ini menyoroti pentingnya pengguna internet di negara-negara anggota ASEAN menerima pemahaman dan perlindungan dari pemerintah terhadap	Parameter dan variable yang digunakan, tujuan penelitian, metode penelitian.

			bahaya ekstremisme siber, radikalisme, dan terorisme. 4) Penelitian ini memperkenalkan konsep *Six-Ware Cyber Security Framework* (SWCSF) sebagai sarana untuk mengatasi masalah ini. Hasil Penelitian: 1) SWCSF diusulkan sebagai konsep awal untuk meningkatkan lingkungan keamanan siber di negara-negara ASEAN. *2)* Penelitia ini menunjukkan bahwa penelitian lebih lanjut diperlukan untuk mengembangkan dan mengimplementasikan SWCSF secara lebih mendalam, terutama dalam enam aspek utama enabler SWCSF: *Brainware, Hardware, Software, Infrastructureware, Firmware,* dan *Budgetware.*	

			3) Kerangka kerja NIST 2014, yang terdiri dari standar, pedoman, dan praktik, disebutkan sebagai referensi untuk mempromosikan perlindungan infrastruktur kritis dan mengurangi risiko siber.	
3.	Arifin Hutomo, Iwan Nofi Yono Putro, Lailatul Qomariyah, Soufi Jayati Ningsih, Ahmad Farid Wadjdi, Andrian Andaya Lestari, Rudy AG Gultom, Susilo Adi Purwantoro, Pujo Widodo, Gita Amperiawan (2021)	*Evaluating the Interoperability of C4ISR System using Cyber Six-ware Framework*	Subjek Penelitian: *1)* Subjek penelitian adalah evaluasi interoperabilitas sistem C4ISR menggunakan *Cyber Six-ware Framework.* Hasil Penelitian: 1) Studi ini menemukan bahwa faktor dominan dalam mengembangkan interoperabilitas C4ISR, menurut penelitian ahli dalam lima tahun terakhir, adalah infrastruktur, perangkat keras, dan *brainware*. 2) Kekuatan signifikan pengembangan interoperabilitas C4ISR di LEN Corp	Parameter dan variable yang digunakan, tujuan penelitian, metode penelitian.

			adalah dalam perangkat lunak dan firmware. 3) Berdasarkan temuan, penelitian ini merekomendasikan bahwa LEN Corp terus menekankan kekuatan "perangkat lunak" selain *firmware* dan *brainware*, sementara juga mengatasi kelemahan dominan dari budgetware.	
4.	Meylia Susiana Dewi Putri (2022)	Analisis Portabilitas Instrumen Pengukuran Sistem Pemerintahan Berbasis Elektronik (SPBE) Dan *Six-Ware Cyber Security Framework* (SWCSF) Untuk Pertahanan Negara	1) Subjek penelitian adalah analisis portabilitas instrumen untuk mengukur Electronic-Based Government Systems (SPBE) dan *Six-Ware Cyber Security* (SWCS) untuk pertahanan nasional. 2) penelitian ini bertujuan untuk menentukan portabilitas instrumen SPBE dan SWCS dan bagaimana portabilitasnya dapat berkontribusi untuk meningkatkan kesadaran keamanan.	Parameter dan variable yang digunakan, tujuan penelitian, metode penelitian.

5.	Rudy Agus Gemilang Gultom, Achmad Farid Wadjdi, Aris Poniman, Sukendra Martha, Kristijarso (2021)	*Sixware Cybersecurity Framework Development To Protect Defense Critical Infrastructure And Military Information Systems*	Subjek Penelitian: 1) Subjek penelitian adalah pengembangan dan penerapan kerangka *Sixware Cybersecurity* (SWCS) untuk menilai kesiapan *cyber defense* dalam organisasi, khususnya di Kementerian Pertahanan dan TNI Indonesia. 2) Studi ini bertujuan untuk menguji efektivitas dan portabilitas kerangka SWCS dalam menilai unit organisasi kecil dengan tugas yang seragam dalam manajemen TI dan operasi siber. Hasil Penelitian: 1) Kerangka kerja SWCS ditemukan praktis, dengan portabilitas dan keandalan yang baik. Hal ini dapat diterapkan secara memadai dan memiliki pola perhitungan sederhana.	Parameter dan variable yang digunakan, tujuan penelitian, metode penelitian.

			2) Implementasi kerangka kerja lebih cocok untuk menilai kesiapan pertahanan siber dalam organisasi atau komunitas yang seragam di bidang TI dan manajemen jaringan atau operasi keamanan siber. 3) Studi ini mendorong penelitian lebih lanjut untuk menguji efektivitas dan portabilitas kerangka SWCS di berbagai organisasi atau komunitas non-TI.	
6.	Nyoman Darmawan, Aris Poniman, Rudy A.G Gultom (2021)	Konsep Pembangunan Teknologi Pertahanan *Cyber Security* Berbasis *Six Ware Framework* Di Markas Komando Pangkalan Tentara Nasional Indonesia Angkatan Laut Palu	Subjek Penelitian: Subjek penelitian adalah pengembangan teknologi pertahanan keamanan siber berdasarkan Kerangka Six Ware di Kepala Pangkalan Angkatan Laut Nasional Indonesia Komando Angkatan Laut Palu. Hasil Penelitian:	Parameter dan variable yang digunakan, tujuan penelitian, metode penelitian.

			Analisis kuantitatif menunjukkan bahwa kemampuan teknologi *cyber defense* berbasis SWCSF di Mako Lanal Palu dikategorikan baik dalam menghadapi ancaman siber. SWCSF memiliki keuntungan dari implementasi yang mudah dalam mengukur kesiapan organisasi terhadap ancaman siber.	
7.	R A G Gultom, A Farid, A A Lestari, C A S Lahallo, R N Akbar (2020)	*Cyber-Based Defense Technology Development of the Six-ware Cyber Framework to Enhance the Implementation of the National Defense System in the City of Batam*	Subjek Penelitian: 1) Subjek penelitian adalah pengembangan dan implementasi "*six-ware cybersecurity framework*" di kota Batam, Indonesia. 2) Studi ini berfokus pada pemahaman implementasi kerangka kerja ini di perusahaan-perusahaan Indonesia dan kesesuaiannya dengan karakteristik perusahaan-perusahaan tersebut. 3) Penelitian ini meneliti kesiapan berbagai perusahaan di Batam,	Parameter dan variable yang digunakan, tujuan penelitian, metode penelitian.

			termasuk BP Batam, Diskominfo, Uniba, NDP, dan AirNav, dalam hal kemampuan dan kesiapan dalam berbagai aspek kerangka kerja. Hasil Penelitian: 1) Analisis kualitatif menunjukkan bahwa BP Batam, Diskominfo, dan Uniba mampu dalam berbagai aspek kerangka kerja, sedangkan NDP lemah dalam aspek *budget-ware* dan AirNav tidak mampu dalam semua aspek. 2) Analisis kuantitatif menunjukkan bahwa Uniba sangat siap dibandingkan dengan lokasi penelitian lainnya, sedangkan NDP adalah yang terlemah karena aspek budget-ware yang kurang. 3) Studi ini menyoroti pentingnya faktor *brainware* dalam keamanan siber, yang lebih berpengaruh daripada perangkat	

			lunak dan perangkat keras, dan menekankan perlunya sinergi antara lembaga pemerintah, perusahaan swasta, dan lembaga pendidikan untuk meningkatkan sistem pertahanan nasional. 4) Penelitian ini menyimpulkan bahwa kerangka *cybersecurity six-ware* bersifat portabel, mudah diimplementasikan, dan dapat dikembangkan menggunakan indeks berbasis perhitungan matematika sederhana.	
8.	Meylia Susiana Dewi Putri, Rudy AG Gultom , Achmad Farid Wadjdi (2023)	*Analysis of SPBE and SWCSF measurement instruments using Flesch Reading Ease for state security*	Subjek Penelitian: 1) Makalah penelitian berfokus pada analisis dua instrumen pengukuran, yaitu *Six-Ware Cyber Security Framework* (SWCSF) dan *Electronic-Based Government System* (SPBE),	Parameter dan variable yang digunakan, tujuan penelitian, metode penelitian.

			dalam konteks keamanan negara dan pencegahan *cybercrime*. 2) Penelitian ini bertujuan untuk mengetahui keterbacaan instrumen ini menggunakan metode Flesch Reading Ease. 3) Penelitian ini menyelidiki apakah individu di tingkat kelas yang berbeda dapat memahami instrumen SPBE dan SWCSF. 4) Studi ini menemukan bahwa kedua instrumen tersebut sangat sulit dipahami oleh responden dari semua tingkatan kelas, kecuali yang berada di tingkat universitas atau individu dengan pengalaman di komputer, internet, dan teknologi lainnya. Hasil Penelitian: 1) Skor Tingkat Kelas *Flesch-Kincaid* untuk instrumen SPBE dan SWCSF	

			masing-masing adalah 19,59 dan 22,72. 2) Skor ini menunjukkan bahwa tingkat pemahaman yang diperlukan oleh kuesioner terdistribusi menggunakan instrumen ini mungkin menantang bagi beberapa responden.	
9.	Seda Demir and Mehmet Fatih Doğuyurt. (2022)	*A comparison of fixed and random effect models by the number of research in the meta-analysis studies with and without an outlier*	Subjek Penelitian: 1) Makalah penelitian membandingkan kinerja Model Efek Tetap (FEM) dan Model Efek Acak (REM) dalam studi meta-analisis. 2) Studi ini menggunakan dataset nyata yang terdiri dari berbagai studi yang meneliti kelelahan emosional guru dalam hal gender. 3) Para peneliti melakukan total 72 meta-analisis menggunakan program R.	Parameter dan variable yang digunakan, tujuan penelitian, objek penelitian, fenomena masalah

			4) Makalah ini berfokus pada perbandingan dua model dalam hal perkiraan ukuran efek umum, tingkat cakupan interval kepercayaan, dan ukuran heterogenitas. 5) Studi ini juga meneliti dampak dari adanya *outlier* dan jumlah studi yang termasuk dalam meta-analisis pada kinerja model. Hasil Penelitian: 1) *Random Effects Model* (REM) ditemukan lebih menguntungkan daripada *Fixed Effect Model* (FEM) saat menganalisis kumpulan data dengan *outlier*. 2) Tanpa *outlier*, ukuran efek umum umumnya diperkirakan serupa untuk kedua model. 3) Meningkatkan jumlah penelitian yang termasuk dalam meta-analisis	

			mengurangi efek *outlier* pada estimasi ukuran efek dan penurunan heterogenitas. 4) Interval kepercayaan mencakup perkiraan ukuran efek di semua kumpulan data dan semua metode. 5) Metode yang digunakan dalam studi meta-analisis dengan 20 studi atau lebih kurang dipengaruhi oleh *outlier run* dalam perkiraan ukuran efek umum.	
10.	Hakan Ulum (2022)	*The efects of online education on academic success: A meta-analysis study*	Subjek Penelitian: 1) Subjek penelitian ini adalah pengaruh pendidikan online terhadap prestasi akademik. Hasil Penelitian: 1) Studi meta-analisis menemukan bahwa ukuran pengaruh pendidikan online pada prestasi akademik berada pada tingkat menengah.	Parameter dan variable yang digunakan, tujuan penelitian, objek penelitian, fenomena masalah

			2) Hasil tes heterogenitas menunjukkan bahwa ukuran efek tidak berbeda dalam hal tingkat kelas, negara, pendekatan pendidikan online, dan moderator kuliah. 3) Studi ini juga bertujuan untuk membandingkan ukuran efek bentuk pendidikan online dekade terakhir dengan apa yang dilakukan hari ini dan di masa depan. 4) Heterogenitas studi yang digabungkan dalam studi meta-analisis dievaluasi menggunakan tes Q dan I2, dan ditentukan bahwa ada tingkat heterogenitas yang tinggi.	

Sumber: Penulis (2023)

2.3 Kerangka Pemikiran

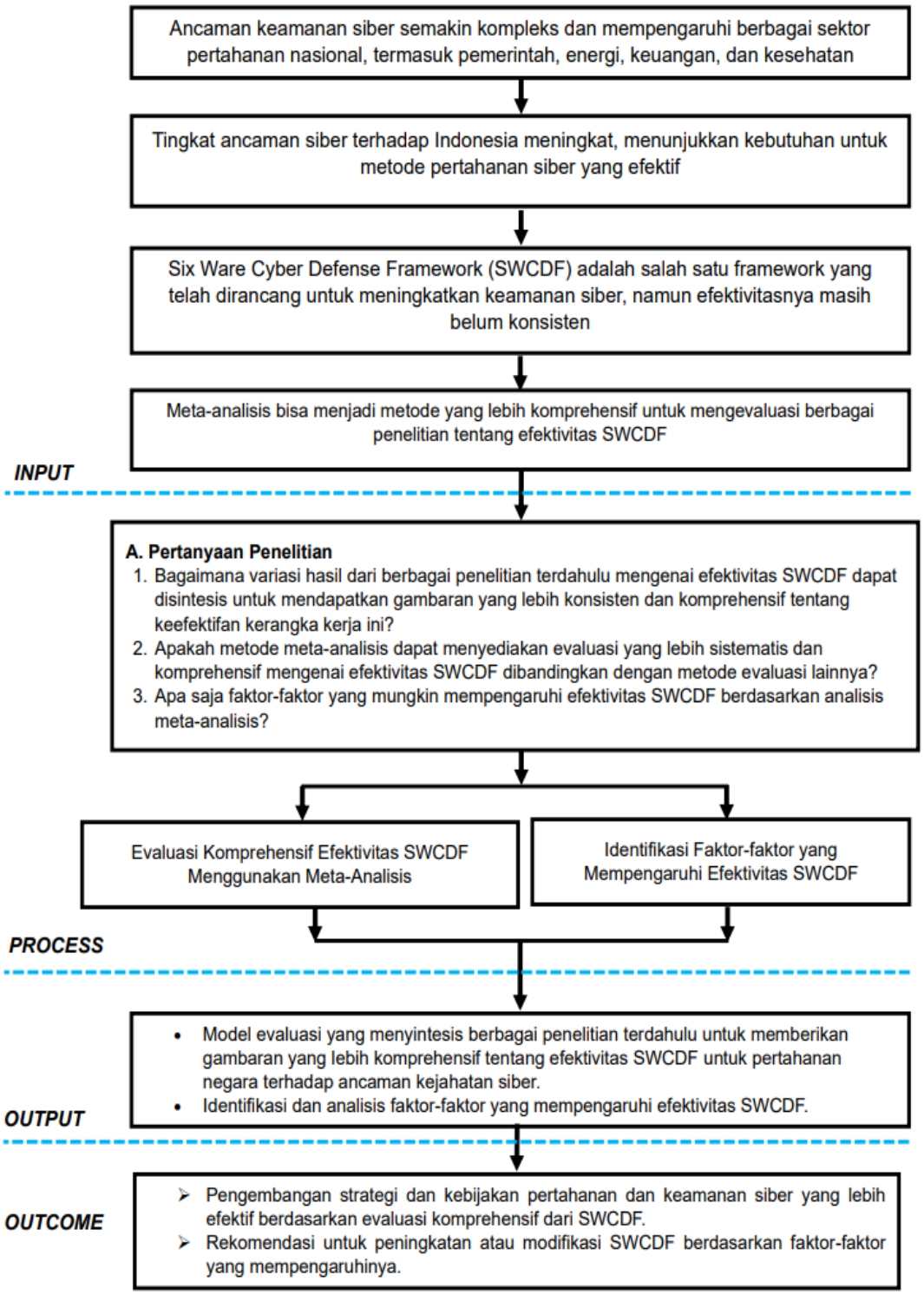
Dalam studi ini, Penulis akan menguraikan struktur pemikiran yang berfungsi sebagai basis konseptual dan teoretis untuk mengarahkan penelitian ini. Struktur pemikiran tersebut akan menyediakan kerangka rujukan yang eksplisit untuk memproses informasi yang telah terkumpul serta menyelesaikan masalah yang menjadi fokus penelitian.

Yang mengacu pada Ancaman siber yang terus meningkat dan kompleksitasnya telah memengaruhi berbagai sektor vital pertahanan nasional Indonesia, termasuk pemerintahan, energi, keuangan, dan kesehatan, meniscayakan kebutuhan mendesak akan metode pertahanan siber yang efektif. Dalam rangka memenuhi kebutuhan ini, Six Ware Cyber Defense Framework (SWCDF) telah dikembangkan sebagai kerangka kerja yang bertujuan untuk memperkuat keamanan siber. Meskipun telah dirancang untuk tujuan ini, konsistensi efektivitas SWCDF masih menjadi subjek diskusi dan analisis yang belum terselesaikan.

Dengan menggunakan meta-analisis sebagai proses utama, penelitian ini akan menciptakan model evaluasi yang menggabungkan temuan dari penelitian terdahulu, memberikan pandangan yang lebih komprehensif tentang efektivitas SWCDF dalam menghadapi ancaman kejahatan siber. Selain itu, penelitian ini bertujuan untuk mengidentifikasi dan menganalisis faktor-faktor yang mempengaruhi efektivitas SWCDF, sehingga hasil dari proses ini diharapkan dapat menghasilkan output yang berupa rekomendasi untuk pengembangan strategi dan kebijakan pertahanan dan keamanan siber yang lebih efektif.

Hasil akhir dari meta-analisis ini tidak hanya akan memperkaya pemahaman kita tentang efektivitas SWCDF tetapi juga akan memberikan dasar bagi pengambilan keputusan yang lebih tepat dalam pembuatan kebijakan, dengan menyarankan peningkatan atau modifikasi pada framework berdasarkan faktor-faktor yang mempengaruhinya. Dengan demikian, output penelitian ini diharapkan dapat mendorong outcome

dalam bentuk peningkatan keandalan dan ketahanan sistem keamanan siber nasional.



Gambar 2. 2 Kerangka Berpikir
Sumber: Penulis (2023