BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan dunia yang sangat cepat terutama di bidang teknologi informasi, keamanan siber menjadi topik yang terus relevan sehingga organisasi akan butuh menilai kesiapan dirinya menghadapi ancaman siber yang terus bereskalasi (Tyagi, 2021). Walaupun banyak kerangka pengukuran keamanan siber, namun *Six Ware Cyber Defense Framework* (SWCDF) dianggap yang lebih portabel dibandingkan kerangka lainnya. SWCDF dikembangkan oleh Universitas Pertahanan sebagai suatu kerangka pengukuran tingkat kesiapan organisasi dalam menghadapi ancaman siber dan telah diklaim oleh beberapa penelitian bahwa kerangka ini memeliki kelebihan kesederhanaannya dan kemudahan implementasinya. Studi ini akan mendalami seluruh hasil riset terdahulu dengan teknik meta-analisis dan mengkomparasikan hasil-hasilnya dengan beberapa kerangka pengukuran yang relevan.

Serangan siber yang semakin meningkat dengan signifikan terhadap pelanggaran keamanan, telah menggaris bawahi kebutuhan akan langkah-langkah keamanan siber yang kuat (Dumitrescu et al., 2020). Integrasi teknologi dalam berbagai aspek masyarakat juga semakin menekankan urgensi keamanan siber (Bajaj & Akhilesh, 2019). Faktor manusia juga berperan penting dalam keamanan siber, karena budaya keamanan yang kuat diperlukan untuk mengelola risiko dengan efektif (Matovu et al., 2020). Kehadiran arsitektur Industrial IoT dan Industrial 4.0 telah meningkatkan kebutuhan akan keamanan siber, terutama dalam domain yang kritis terhadap keselamatan (Rathod & Hämäläinen, 2020). Insiden keamanan siber memiliki potensi dampak negatif yang luas, termasuk pada bisnis, masyarakat, dan pertahanan negara, sehingga mengedepankan prioritas pada keamanan siber sangatlah penting.

Perkembangan pertahanan siber telah menjadi masalah nasional maupun global karena meningkatnya ancaman yang ditimbulkan oleh *cybercrime* dan *cyber warfare*. Kemajuan teknologi yang pesat dalam domain digital telah menyebabkan munculnya bentuk-bentuk baru ancaman siber, seperti *ransomware* dan senjata siber, yang berpotensi menyebabkan kerusakan signifikan pada skala global (Koch & Golling, 2018; Sabbagh, 2019). Kerentanan dalam infrastruktur siber dan potensi penggunaan senjata siber sembarangan menimbulkan kekhawatiran tentang kecukupan solusi hukum dan strategis saat ini (Sharikov, 2019). Ada kebutuhan akan kemampuan pertahanan siber nasional yang komprehensif dan kerja sama internasional untuk mengatasi tantangan ini (Clark & Hakim, 2017; Zhuravel, 2020). Dampak kejahatan dunia maya dan potensi perang siber menyoroti urgensi memprioritaskan keamanan informasi dan berinvestasi dalam penelitian dan pengembangan solusi keamanan siber bernilai tinggi.

Gambar 1. 1 Jumlah Serangan Siber Di Indonesia (2018-2022)
Sumber: dataindonesia.id

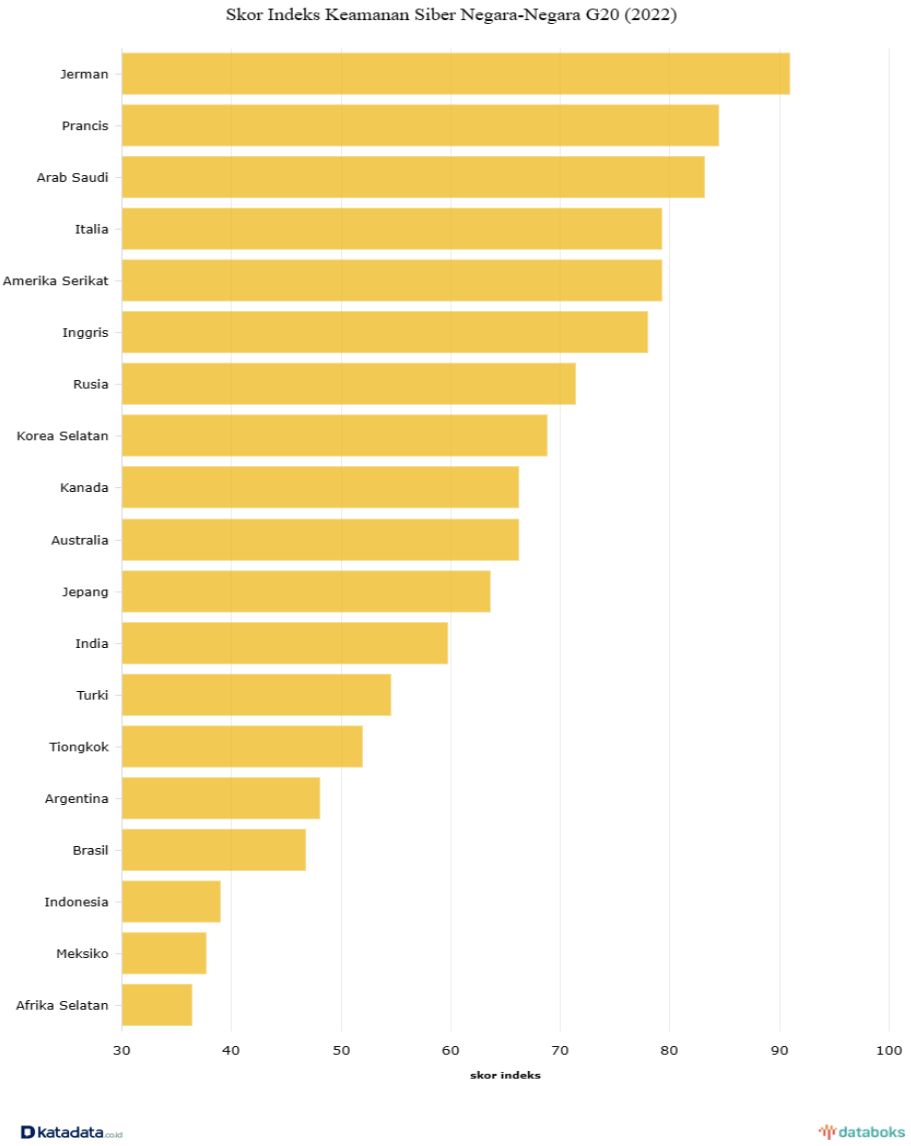
Badan Siber dan Sandi Negara (BSSN) mencatat bahwa pada tahun 2022, Indonesia mengalami sebanyak 370,02 juta serangan siber. Angka ini menunjukkan peningkatan sebesar 38,72% dibandingkan tahun

sebelumnya yang mencapai 266,74 juta serangan siber di dalam negeri. Jika melihat tren dalam empat tahun terakhir, jumlah serangan siber di tingkat nasional cenderung berfluktuasi. Pada tahun 2020, terjadi lonjakan menjadi 316,17 juta serangan, kemudian mengalami penurunan sebesar 15,63% menjadi 266,74 juta serangan pada tahun 2021. Namun, jumlah serangan kembali meningkat pada tahun 2022. Secara khusus, serangan siber terbanyak pada tahun 2022 berasal dari dalam negeri, mencapai 84,86 juta serangan. Sementara itu, serangan dari India dan Bangladesh masing-masing mencapai 80,36 juta dan 27,99 juta serangan. Dilihat dari sektor yang menjadi target, administrasi pemerintahan merupakan yang paling banyak diserang dengan 284,09 juta kasus pada tahun 2022. Sementara sektor energi dan sumber daya manusia (SDM) juga mengalami 2,38 juta serangan. Sektor keuangan di Indonesia juga terkena serangan sebanyak 5,72 juta kali, sementara sektor kesehatan mengalami 850.281 serangan siber (Febriana Sulistya Pratiwi, 2023).

Selain itu, terdapat isu serius terkait kebocoran data pribadi warga negara Indonesia (WNI). Data paspor WNI sebanyak 34 juta diduga bocor dan dijual. Data yang bocor meliputi nomor paspor, tanggal berlaku, nama lengkap, tanggal lahir, dan jenis kelamin. Kejadian ini bukan yang pertama kalinya terjadi di Indonesia, dengan 79 kasus serupa sejak tahun 2019. Bahkan, Kementerian Komunikasi dan Informatika (Kominfo) mencatat 35 kasus kebocoran data di Indonesia hanya dalam enam bulan pertama tahun 2023, melebihi jumlah kasus yang terjadi selama tiga tahun sebelumnya, yaitu dari 2019 hingga 2021 (Amelia Shinta, 2022).

Beberapa kasus serangan siber yang pernah terjadi di Indonesia juga mencakup Peretasan situs BPJS Kesehatan pada Mei 2021, yang mengakibatkan data 279 juta penduduk Indonesia bocor dan dijual, kebocoran data asuransi BRI Life pada Juli 2021, yang memengaruhi 2 juta data nasabah, Serangan deface terhadap website Sekretariat Kabinet RI, Serangan DDoS terhadap situs DPR RI pada Oktober 2020, kebocoran data dari aplikasi *Electronic Health Alert* (e-HAC) Kemenkes RI pada Juli

2021, peretasan pada Tiket.com dan Citilink pada Oktober 2016, dengan kerugian mencapai miliaran rupiah, kebocoran data pengguna Tokopedia pada Mei 2020, memengaruhi 91 juta akun pengguna dan pembobolan database Polri pada November 2021, dengan data *log in* dan informasi pribadi yang dicuri (Amelia Shinta, 2022). Semua kasus ini menunjukkan bahwa serangan siber merupakan masalah serius di Indonesia, dan upaya perbaikan keamanan siber sangat diperlukan untuk melindungi data pribadi dan infrastruktur negara.



Gambar 1. 2 Laporan National Cyber Security Index (NCSI)
Sumber: Indeks Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20 (katadata.co.id)

Laporan *National Cyber Security Index* (NCSI) mencatat bahwa pada 2022, skor indeks keamanan siber Indonesia tercatat rendah, menempatkannya di peringkat ketiga terendah di antara negara-negara G20. Secara global, Indonesia menempati peringkat ke-83 dari 160 negara dalam laporan tersebut (Cindy Mutia Annur, 2022). Serangan siber yang berhasil dapat mengganggu infrastruktur penting, seperti pasokan listrik dan sistem transportasi, dengan dampak yang melumpuhkan ekonomi dan kehidupan masyarakat. Hal ini juga berdampak serius pada pertahanan negara, karena mengganggu konektivitas krusial dan kemampuan logistik yang penting dalam situasi darurat atau konflik militer. Dalam situasi semacam itu, respons terhadap ancaman luar dapat terhambat.

Jaringan militer dan infrastruktur komunikasi rentan terhadap serangan siber yang sering, yang dapat menyebabkan gangguan dalam komunikasi antar unit dan penurunan efisiensi operasional (Sedaghat & Gini, 2019). Hal ini tidak hanya mengurangi kemampuan pertahanan suatu negara untuk menanggapi ancaman tetapi juga merusak kepercayaan publik terhadap pemerintah, berpotensi memicu ketidakstabilan sosial dan politik yang lebih luas (Clark & Hakim, 2017). Untuk mengatasi masalah ini, sangat penting bagi pemerintah, masyarakat, dan sektor swasta untuk bekerja sama. Peningkatan langkah-langkah keamanan siber, seperti meningkatkan literasi dan kesadaran siber, menerapkan praktik keamanan yang baik, dan melaporkan keluhan siber kepada otoritas terkait, diperlukan untuk menciptakan dunia maya yang aman (Stockburger, 2016). Kegagalan untuk menjaga keamanan di sektor ini dapat memberikan peluang bagi entitas asing atau kelompok teroris untuk melakukan serangan terkoordinasi, yang menimbulkan ancaman signifikan terhadap keamanan nasional (Qureshey, 2015).

Tantangan utama dalam mengukur keamanan siber adalah meningkatnya beragam ancaman. Keamanan siber terus berubah dengan

perkembangan teknologi dan taktik serangan (Dumitrescu et al., 2020) (Herrmann & Pridöhl, 2020). Hal ini semakin diperumit oleh munculnya perangkat yang terhubung ke internet, termasuk *Internet of Things* (IoT), yang meningkatkan potensi titik serangan (Rathod & Hämäläinen, 2020). Selain itu, keterbatasan metrik juga menjadi tantangan. Meskipun ada banyak alat dan metrik untuk mengukur keamanan siber, seringkali tidak memberikan gambaran yang komprehensif (Ahmed & A. Hikal, 2019). Sebuah organisasi mungkin memiliki tingkat keberhasilan deteksi yang tinggi tetapi lambat dalam menanggapi insiden, yang dapat memiliki dampak besar (Tomsu, 2021). Banyak metrik bersifat kuantitatif dan tidak memperhitungkan aspek kualitatif seperti dampak reputasi atau kepercayaan pelanggan.

Karena itu, para profesional dan Penulis di bidang keamanan siber perlu terus mengembangkan metode pengukuran yang lebih efektif. Six *Ware Cyber Defense Framework* (SWCDF) adalah kerangka kerja yang dirancang untuk meningkatkan pertahanan siber dan melindungi infrastruktur dan sistem informasi militer (Meylia Susiana Dewi Putri et al., 2023). Terdiri dari enam komponen utama SWCDF yang disebut sebagai "*ware*", yaitu *Brainware, Hardware, Software, Infrastructureware, Firmware,* dan *Budgetware* kerangka kerja ini menawarkan pendekatan standar untuk perlindungan jaringan komputer dan dapat digunakan untuk merancang sistem pertahanan siber yang efektif untuk infrastruktur penting (Susiana et al., 2023). SWCDF menyoroti pentingnya faktor manusia dalam lingkungan keamanan jaringan dan memberikan solusi untuk mengelola risiko dan analisis dalam jaringan komputer (Gultom et al., 2018a). Dengan menerapkan SWCDF, organisasi dapat meningkatkan lingkungan keamanan jaringan dan meningkatkan kesadaran dalam menghadapi ancaman (Susiana et al., 2023). Namun, perlunya tinjauan lebih lanjut terhadap efektivitas kerangka kerja ini untuk mengukur tingkat keamanan siber. Hal ini akan memberikan wawasan berharga bagi para peneliti,

praktisi, dan pembuat kebijakan di bidang keamanan siber (Hutomo et al., 2021).

Sejauh ini, banyak penelitian telah dilakukan untuk menguji efektivitas dari SWCDF dalam konteks keamanan siber. SWCDF termasuk meningkatkan ketahanan keamanan jaringan dan melawan aktivitas ekstremisme kejahatan di dunia maya. SWCDF termasuk menyediakan solusi keamanan jaringan utama dan meningkatkan ketahanan keamanan jaringan organisasi. Kerangka pengukuran SWCDF memiliki beberapa keunggulan. Pertama, praktis dan memiliki portabilitas yang baik, sehingga mudah untuk menerapkan dan mengukur kesiapan organisasi terhadap ancaman siber (M. Susiana, 2023). Kedua, menyediakan pendekatan komprehensif dengan mempertimbangkan enam komponen: *Brainware, Hardware, Software, Infrastructureware, Firmware, dan Budgetware* (Agus Gemilang Gultom et al., 2021). Ini memastikan bahwa semua aspek pertahanan siber diperhitungkan, termasuk sumber daya manusia, teknologi, infrastruktur, dan alokasi anggaran. Selain itu, kerangka kerja ini cocok untuk menilai kesiapan pertahanan siber dalam organisasi atau komunitas yang seragam di bidang TI dan manajemen jaringan atau operasi keamanan siber (Darmawan et al., 2021). Ini dapat diterapkan secara efektif baik di organisasi militer dan non-militer, membuatnya serbaguna dan dapat beradaptasi dengan konteks yang berbeda (Agus et al., 2022; Gultom et al., 2020). Secara keseluruhan, kerangka pengukuran SWCDF menawarkan keandalan yang baik, portabilitas tinggi, dan kesesuaian untuk menilai unit organisasi dengan skala besar sampai organisasi kecil dalam manajemen TI dan operasi siber, pendekatan praktis dan komprehensif untuk menilai dan meningkatkan kemampuan pertahanan dunia maya organisasi. Portabilitas instrumen merupakan aspek krusial dalam mengevaluasi sejauh mana suatu model atau sistem pengukuran dapat dengan mudah diterapkan, dan pada akhirnya, ini juga berhubungan dengan seberapa efektif dan efisien penggunaan sumber daya dalam pelaksanaannya (M. Susiana, 2023). Hasilnya,

bagaimanapun, menunjukkan variasi yang signifikan. Beberapa studi menyatakan bahwa SWCDF adalah metode yang sangat efektif dan holistik dalam mengukur dan menangani masalah keamanan siber (Gultom et al., 2020). Bagaimana Meta-Analisis Bisa Menggabungkan Berbagai Temuan untuk Memberikan Kesimpulan yang Lebih Kuat?

Dalam konteks ini, meta-analisis muncul sebagai sebuah metode yang sangat berguna. Melalui meta-analisis dapat menggabungkan data dan temuan dari berbagai studi yang telah dilakukan terkait efektivitas SWCDF. Ini tidak hanya akan meningkatkan ukuran sampel secara keseluruhan, tetapi juga akan memungkinkan untuk mengidentifikasi pola, konsistensi, atau anomali yang mungkin tidak jelas dalam studi individu (Fujs et al., 2019).

Lebih jauh lagi, meta analisis memungkinkan untuk melakukan analisis statistik yang lebih canggih, seperti mengidentifikasi faktor-faktor yang mungkin mempengaruhi efektivitas SWCDF (Groß, 2021). Misalnya, apakah efektivitas SWCDF dipengaruhi oleh jenis industri, ukuran perusahaan, atau tingkat keahlian tim keamanan siber? Jawaban atas pertanyaan-pertanyaan ini akan memberikan wawasan yang lebih mendalam tentang di mana dan kapan SWCDF paling efektif, dan di mana mungkin memerlukan peningkatan atau modifikasi (Lu, 2018).

Oleh karena itu, melalui metode meta-analisis, penelitian ini bertujuan untuk menawarkan sebuah evaluasi yang lebih komprehensif dan sistematis dari efektivitas SWCDF dalam konteks keamanan siber. Hasil dari penelitian ini diharapkan akan membantu praktisi, pengambil keputusan, dan Penulis lain dalam memahami potensi penuh serta keterbatasan dari SWCDF sebagai alat pengukuran keamanan siber.

1.2 Identifikasi Masalah

Berdasarkan konteks yang telah diuraikan pada sub bagian latar belakang sebelumnya, penulis telah mengenali beberapa isu kritis yang akan diangkat sebagai fokus dalam tesis penelitian ini:

a. Kebutuhan Metodologi Penelitian yang Lebih Kuat: Mengingat variasi besar dalam hasil penelitian sebelumnya, ada kebutuhan untuk metode yang lebih sistematis dan komprehensif, seperti meta-analisis, untuk memahami efektivitas sebenarnya dari SWCDF.
b. Keefektifan SWCDF Masih Belum Konsisten: Penelitian yang ada menunjukkan hasil yang bervariasi mengenai efektivitas SWCDF, membuatnya sulit untuk menentukan sejauh mana kerangka kerja ini dapat diandalkan.
c. Beragamnya Ancaman Keamanan Siber: Keamanan siber tidak hanya dipengaruhi oleh faktor teknis tapi juga oleh faktor manusia, perkembangan teknologi, dan jenis industri. Hal ini membuat pengukuran keamanan siber menjadi lebih kompleks.

1.3 Pembatasan Masalah

Berdasarkan konteks dan permasalahan yang telah dijelaskan sebelumnya, menetapkan batasan masalah dalam penelitian ini menjadi krusial untuk mempertahankan integritas dan relevansi analisis serta kesimpulan yang akan diambil. Tujuannya adalah untuk mencegah deviasi dari fokus penelitian dan menargetkan aspek-aspek spesifik yang akan diselidiki. Berikut beberapa batasan masalah yang perlu dipertimbangkan dalam penelitian ini:

a. Metodologi Penelitian: Penelitian ini akan terfokus pada penggunaan meta-analisis sebagai metode untuk mengevaluasi efektivitas SWCDF. Oleh karena itu, penelitian ini tidak akan memasukkan metode evaluasi lain yang bisa digunakan untuk mengukur efektivitas SWCDF.
b. Variabilitas Hasil Penelitian: Konsentrasi utama akan diberikan pada studi-studi yang telah mempublikasikan data mengenai efektivitas SWCDF, yang memungkinkan dilakukannya analisis statistik. Studi yang tidak menyajikan data yang cukup untuk meta-analisis akan dikecualikan.

1.4 Rumusan Masalah

Berdasarkan latar belakang dan konteks yang telah disajikan di atas, beberapa rumusan masalah yang bisa diajukan dalam penelitian ini adalah:

a. Bagaimana variasi hasil dari berbagai penelitian terdahulu mengenai efektivitas SWCDF?
b. Apa saja faktor-faktor yang mempengaruhi efektivitas SWCDF?
c. Bagaimanakah efektivitas dan sensitivitas antar komponen SWCDF?

1.5 Tujuan Penelitian

Berdasarkan permasalahan yang telah dirumuskan, studi ini diarahkan untuk mencapai tiga sasaran utama:

a. Evaluasi Komprehensif Efektivitas SWCDF: Tujuan utama dari penelitian ini adalah untuk mengevaluasi efektivitas SWCDF dalam konteks keamanan siber menggunakan metode meta-analisis. Ini akan mencakup penilaian dari berbagai penelitian yang telah ada untuk memberikan gambaran yang lebih komprehensif dan konsisten tentang efektivitas kerangka kerja ini.
b. Identifikasi Faktor-faktor yang Mempengaruhi Efektivitas SWCDF: Penelitian ini juga bertujuan untuk mengidentifikasi faktor-faktor yang mungkin mempengaruhi efektivitas SWCDF, seperti jenis industri, ukuran perusahaan, atau tingkat keahlian tim keamanan siber, berdasarkan data yang dikumpulkan melalui meta-analisis.
c. Pembandingan efektivitas dan sensitivitas antar komponen SWCDF: Meskipun fokus utama adalah pada meta-analisis, tujuan sekunder adalah untuk membandingkan hasil efektivitas dan sensitivitas antar komponen SWCDF, untuk menentukan kestabilan antar komponen SWCDF dan memberikan wawasan yang lebih komprehensif dan sistematis.

1.6 Manfaat Penelitian

Berikut ini adalah manfaat yang diharapkan dari penelitian ini:

1.6.1 Manfaat Teoritis

1) Menawarkan kontribusi pada teori dan konsep dalam keamanan siber, khususnya mengenai efektivitas dan aplikabilitas SWCDF.
2) Memperdalam pemahaman tentang pentingnya meta-analisis dalam sintesis literatur keamanan siber, sehingga memungkinkan Penulis dan praktisi memahami berbagai aspek yang mempengaruhi efektivitas SWCDF.
3) Memajukan teori tentang faktor-faktor yang mempengaruhi efektivitas alat dan metrik keamanan siber, memungkinkan penelitian lebih lanjut dan pengembangan metrik yang lebih tepat.

1.6.2 Manfaat Praktis

1) Memberikan rekomendasi kepada pemangku kebijakan, khususnya di bidang keamanan siber, tentang bagaimana efektivitas SWCDF dapat ditingkatkan berdasarkan analisis komprehensif dalam lingkungan kementrian pertahanan RI, TNI dan instansi K/L pemerintahan, instansi Pendidikan, swasta dan instansi lainnya.
2) Menyediakan wawasan yang bisa diaplikasikan dalam praktik keamanan siber, misalnya dalam merancang atau menyesuaikan alat dan metrik yang lebih efektif untuk mengukur dan meningkatkan keamanan siber di kementerian/Lembaga pertahanan RI, TNI, dan Lembaga atau industry pemerintah atau swasta, instansi Pendidikan, indrustri kreatif dan instansi lainnya.
3) Menyajikan analisis yang dapat dijadikan referensi oleh perusahaan dan organisasi untuk meningkatkan keamanan siber, terutama dalam memilih atau menyesuaikan *framework* yang akan digunakan di kementerian/Lembaga pertahanan RI, TNI, dan

Lembaga atau industry pemerintah atau swasta instansi Pendidikan, indrustri kreatif dan instansi lainnya.