BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan penelitian yang telah dilakukan mengenai efektivitas SWCDF *(Software, Hardware, Firmware, Brainware, Infrastructureware, dan Budgetware* dalam Cyber Defense Framework) dalam konteks keamanan siber, serta mempertimbangkan berbagai studi dan meta-analisis yang telah dilakukan, penelitian ini memberikan kontribusi penting dalam pemahaman dan penerapan strategi pertahanan siber. Hal ini tidak hanya meningkatkan pemahaman tentang bagaimana berbagai komponen SWCDF dapat diterapkan secara efektif dalam berbagai konteks institusional, tetapi juga memberikan wawasan baru dalam penerapan kerangka kerja ini untuk meningkatkan pertahanan siber secara nasional. Oleh karena itu, dapat ditarik kesimpulan sebagai berikut.

1. Variasi Hasil dari Berbagai Penelitian Terdahulu Mengenai Efektivitas SWCDF (*Software, Hardware, Firmware, Brainware, Infrastructureware, Budgetware*):

   a) Efektivitas SWCDF secara umum: SWCDF secara keseluruhan memiliki dampak positif yang signifikan dalam meningkatkan pertahanan siber di berbagai jenis instansi. Khususnya, di sektor Pertahanan Negara, SWCDF menunjukkan efektivitas yang paling tinggi. *Brainware* (BRW) memiliki pengaruh signifikan terhadap efektivitas pertahanan siber nasional di semua jenis instansi, dengan Instansi Pendidikan menonjol dengan point estimate tertinggi. Variabilitas antar instansi menunjukkan pentingnya penyesuaian strategi pertahanan siber yang spesifik untuk setiap instansi. Software (SW) memiliki peran penting dan signifikan dalam peningkatan pertahanan siber di semua jenis instansi, khususnya efektif dalam sektor Pertahanan Negara. SW memiliki point estimate 81.06

(standard error 2.1779) dan 95% confidence interval 76.7891-85.3263 di BUMN, dan point estimate tertinggi 93.57 di Pertahanan Negara.

b) Variasi dalam efektivitas: Terdapat variasi dalam hasil yang diamati di berbagai subgrup, menunjukkan bahwa faktor kontekstual spesifik mungkin mempengaruhi bagaimana SWCDF diimplementasikan dan dikelola di setiap instansi.

2. Faktor-faktor yang Mempengaruhi Efektivitas SWCDF:

a) Variabilitas dalam efektivitas SWCDF antar instansi mengindikasikan bahwa konteks spesifik dari setiap instansi dan cara penerapan komponen SWCDF (seperti *Firmware* dan *Brainware*) memainkan peran penting dalam menentukan efektivitasnya.

b) Pentingnya penyesuaian strategi pertahanan siber yang spesifik untuk setiap instansi.

3. Efektivitas dan sensitivitas antar komponen SWCDF:

a) Kesimpulan studi mendukung penggunaan SWCDF dalam berbagai konteks pertahanan siber dengan pertimbangan terhadap kekhususan instansi. SWCDF menunjukkan efektivitas yang signifikan secara statistik dalam meningkatkan pertahanan siber di berbagai jenis instansi, dengan Instansi Pendidikan dan Pertahanan Negara menunjukkan efektivitas tertinggi. Hal ini menunjukkan bahwa SWCDF sangat berguna dalam konteks tersebut, meskipun ada variasi dalam efektivitas yang diamati terutama di subgrup Industri Ekonomi Kreatif.

b) Uji publikasi bias menunjukkan tidak adanya bias yang signifikan dalam penelitian terkait SWCDF, menambah kepercayaan pada hasil meta-analisis. Hal ini berlaku untuk komponen-komponen seperti

BRW, SW, HW, ISW, FW, dan BGW, serta SWCDF secara keseluruhan.

c) *Software* (SW) dan *Hardware* (HW) teridentifikasi sebagai elemen paling efektif dalam SWCDF, tetapi efektifitasnya menunjukkan variasi yang lebih besar berdasarkan beberapa kondisi yang di artikan memiliki sensitivitas yang rendah dibandingkan dengan komponen lainnya. Sementara itu, Budgetware (BGW) dan Infrastructureware (ISW) menawarkan efisiensi yang lebih konsisten, yang krusial untuk stabilitas keamanan siber. Temuan ini menegaskan pentingnya memperhatikan sensitivitas komponen 'ware' dalam pengembangan dan aplikasi strategi pertahanan siber, untuk memastikan keseimbangan efisiensi, keandalan, dan daya tahan terhadap ancaman siber.

Secara keseluruhan, hasil penelitian menunjukkan bahwa SWCDF merupakan kerangka kerja efektif dalam konteks keamanan siber, dengan efektivitas yang bervariasi tergantung pada konteks spesifik setiap instansi dan cara penerapan komponennya. Penelitian lebih lanjut diperlukan untuk memahami faktor-faktor yang menyebabkan perbedaan ini dan untuk mengoptimalkan penerapan SWCDF di berbagai instansi.

5.2 Saran

Berdasarkan hasil dan analisis dalam penelitian ini mengenai efektivitas *Six Ware Cyber Defense Framework* (SWCDF) dalam konteks keamanan siber, berikut adalah beberapa saran untuk penelitian lebih lanjut dan pengembangan praktik di bidang ini:

1. Penyesuaian SWCDF Berdasarkan Konteks Instansi: SWCDF menunjukkan efektivitas yang beragam di berbagai jenis instansi. Penelitian lebih lanjut diperlukan untuk memahami bagaimana faktor kontekstual spesifik dari setiap instansi mempengaruhi efektivitas komponen SWCDF. Ini termasuk mengkaji cara penerapan SWCDF

dan integrasi komponennya dalam infrastruktur keamanan siber yang ada.

2. Fokus pada Variabilitas dan Faktor Pengaruh: Variabilitas dalam efektivitas SWCDF antar instansi menunjukkan adanya faktor lain yang mempengaruhi kinerjanya. Penelitian lebih lanjut dapat mengeksplorasi faktor-faktor ini untuk mengidentifikasi dan mengatasi hambatan yang mungkin mengurangi efektivitas SWCDF.
3. Investigasi Lebih Mendalam pada Komponen Individual SWCDF: Analisis menunjukkan bahwa setiap 'ware' dalam SWCDF memiliki pengaruh yang signifikan dalam peningkatan pertahanan siber. Studi lebih lanjut dapat difokuskan pada pengukuran di dalam organisasi yang cukup besar agar SWCDF dapat di evaluasi untuk pengembangan di semua ukuran organisasi dari kecil sampai menengah karena selama ini SWCDF banya di gunakan pada organisasi kecil sampei menengah untuk ukuran populasinya sehingga setiap komponen dapat dioptimalkan dan diintegrasikan dengan efektif dalam strategi pertahanan siber secara keseluruhan.