BAB 2

TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 Sistem Petahanan Negara

Setiap negara memiliki sebuah sistem pertahanan negara yang mengatur mengenai perlindungan dan keamanan negara tersebut. Indonesia memiliki sistem pertahanan negara yang bernama sistem pertahanan rakyat semesta (Sishanta). Hal tersebut diatur pada Pasal 30 Ayat 2 Undang-Undang Dasar 1945. Sistem pertahanan rakyat semesta memiliki makna yaitu melibatkan seluruh rakyat dan sumber daya nasional, sarana dan prasarana serta semua wilayah negara sebagai satu kesatuan. Makna lain dari semesta yaitu pertahanan negara Indonesia dilakukan untuk seluruh wilayah Indonesia dengan tujuan negara yang berbentuk kepulauan ini memiliki suatu pertahanan yang kokoh. Pertahanan negara termasuk dalam bagian dari fungsi pemerintahan pada suatu negara yang memiliki tujuan untuk mencapai tujuan nasional. Ciri dari sebuah sistem pertahanan semesta adalah kerakyatan, kesemestaan, serta kewilayahan. Kerakyatan yaitu memiliki arti pandangan mengenai pertahanan yang diabadikan bersama rakyat dengan tujuan kepentingan seluruh rakyat. Kesemestaan dapat diartikan sebagai memanfaatkan semua sumber daya dan sarana prasarana untuk usaha pertahanan. Kewilayahan menjelaskan mengenai penerapan kekuatan pertahanan diadakan sepenuhnya di Indonesia sesuai keadaan geografis Indonesia yaitu negara maritim (Kementerian Pertahanan Republik Indonesia, 2015).

Saat ini, pertahanan negara tidak hanya melindungi matra darat, laut dan udara. Perkembangan teknologi dengan memanfaatkan teknologi informasi dan informasi (TIK) yang semakin pesat dan penggunaan internet

yang terus meningkat membuat matra siber menjadi hal yang perlu dilindungi. Ruang siber dapat menjadi sebuah ancaman dan potensi gangguan bagi negara Indonesia. Saat ini, perang siber dapat dikatakan sudah berlangsung yang dibuktikan dengan adanya informasi palsu sehingga menggiring opini masyarakat yang berdampak pada ketakutan dan kecemasan. Sesuai dengan UU RI Nomor 3 Tahun 2002 mengenai Pertahanan Negara yang dibagi menjadi ancaman militer dan non-militer. Urgensi pertahanan siber bertujuan dalam mengantisipasi munculnya ancaman dan serangan siber dan menjelaskan posisi pertahanan saat ini, sehingga diperlukannya kesiapan dan ketanggapan dalam menghadapi ancaman serta memiliki kemampuan untuk memulihkan dampak yang terjadi dari serangan pada ruang siber.

Bergeraknya perkembangan lingkungan strategis secara dinamis memberikan dampak pada perubahan kondisi ancaman yang menjadi kompleks dan berdampak langsung pada pertahanan negara. Berkembangnya teknologi saat ini dapat meningkatkan ancaman yang menjadi semakin kompleks dan multidimensional yaitu ancaman militer, ancaman nirmiliter dan ancaman hibrida yang dikelompokan menjadi ancaman nyata dan belum nyata. Dengan kompleksitas ancaman tersebut maka salah satu penyelesaiannya dengan perlunya pertahanan negara membangun kesatuan dan keterpaduan antara pertahanan militer dan pertahanan nirmiliter untuk menjadikan pertahanan Indonesia yang andal, kuat, disegani dan memiliki daya tangkal yang tinggi.

2.1.2 Sistem Pemerintahan Berbasis Elektronik

Indonesia memasuki era Revolusi Industri 4.0 dan Internet of Things (IoT) serta di tengah maraknya perkembangan masyarakat Society 5.0 menyebabkan masyarakat memiliki ketergantungan terhadap teknologi informasi dan komunikasi yang terus meningkat. Transformasi digital dalam pemerintahan sudah menjadi suatu keharusan untuk dilaksanakan pada

berbagai kegiatan pemerintahan (Pepres no. 132 Tahun 2022). Kegiatan ekonomi, pelayanan publik, politik, keamanan bahkan pertahanan kini semakin terkomputerisasi, otonom, dan terintegrasi sehingga menjadi lebih mudah, efektif, dan efisien. Salah satu pelayanan publik di Indonesia yang saat ini sedang dikembangkan adalah e-Government atau yang diketahui sebagai Sistem Pemerintah Berbasis Elektronik (SPBE). Pelaksanaan pengembangan SPBE yang bertujuan mengembangkan tranformasi digital di pemerintahan sesuai dengan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Tetapi, SPBE di Indonesia dinilai hanya sebagai sebuah proyek yang cukup atas kepemilikan website dan tidak peduli terhadap optimalisasi pemanfaatan SPBE. Berdasarkan United Nations e-Government Survey (2020), Indonesia berada pada peringkat ke-88 di dunia dalam kemajuan e-Government. Tujuan dikembangkannya SPBE adalah untuk mempermudah interaksi antara pemerintah dan masyarakat melalui website pemerintah. SPBE dalam mencapai keberhasilannya tidaklah mudah. Hal ini melibatkan pendekatan multidimensi, memikirkan kembali dan merekayasa ulang proses pemerintah, mengubah budaya organisasi, menetapkan undang-undang pemerintahan yang baru. Untuk mencapai hal tersebut diperlukannya koordinasi banyak kegiatan unit pemerintah dan kerjasama yang erat antara pegawai pemerintah, manajer dan spesialis IT serta masyarakat (Ziemba dkk, 2015).

SPBE merupakan pemanfaatan teknologi informasi, internet dan komunikasi yang dikembangkan oleh pemerintah dengan tujuan mentransformasikan hubungan pemerintah dengan masyarakat, pelaku dunia bisnis, dan lembaga pemerintah lainnya (Bank Dunia, 2002). Berdasarkan Peraturan Presiden Republik Indonesia nomor 132 Tahun 2022 menyatakan bahwa SPBE merupakan penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi (TIK) dengan tujuan memberikan layanan kepada pengguna SPBE. Dalam pengimplementasian

SPBE di pemerintahan, terdapat 7 indikator yang menjadi pengukuran dari insrumen SPBE. Indikator tersebut dapat dilihat pada Tabel 2.1.

Tabel 2.1. Indikator pada Instrumen SPBE (Trishadiatmoko dkk, 2021)

No.	Indikator
1.	Kebijakan Tata Kelola
2.	Kebijakan Layanan
3.	Kelembagaan
4.	Strategi dan Perencanaan
5.	Teknologi Informasi dan Komunikasi
6.	Layanan Administrasi
7.	Layanan Publik

Penerapan SPBE di era sekarang sangat diperlukan untuk menjamin terwujudnya transparansi, efisiensi, kecepatan penyampaian informasi, keterjangkauan pelayanan pemerintah kepada masyarakat dan dunia usaha (Septiani, 2020). Hal itu membuktikan bahwa pengembangan SPBE pada pemerintahan merupakan salah satu indikator pembangunan. Menurut Yalia (2011), beberapa contoh implementasi dari SPBE adalah pelayanan pajak, pelayanan pendaftaran warga negara, pengurusan perizinan bangunan dan kendaraan, serta lainnya. Arsitektur yang dibangun pada SPBE Nasional merupakan pedoman yang digunakan untuk perkembangan arsitektur SPBE Pusat dan arsitektur SPBE Daerah. Referensi arsitektur yang digunakan pada SPBE pusat dan daerah adalah sebagai berikut (Perpres No. 132 tahun 2022) :

a. Referensi arsitektur proses bisnis.
b. Referensi arsitektur data dan informasi.
c. Referensi arsitektur layanan SPBE .
d. Referensi arsitektur aplikasi SPBE.

Dengan pembangunan dan perkembangan arsitektur pembangunan SPBE di instansi pusat, daerah dan nasional yang selaras sehingga akan memudahkan untuk dilakukannya pengintegrasian yang diperlukan. Pelaksanaan SPBE yang terus berkembang merupakan tujuan sebagai wahana transformasi digital menuju Indonesia 4.0 pada tahun 2040.

2.1.3 Six-Ware Cyber Security

Perkembangan teknologi yang semakin pesat membuat dunia memasuki era digital yang mengharuskan adanya konektivitas jaringan internet. Perkembangan teknologi digital tentu memiliki dampak negatif yang ditimbulkan salah satunya kejahatan cyber. Konsep Six-Ware Cyber Security merupakan sebuah konsep dengan tujuan agar memiliki kesiapan dalam timbulnya ancaman cyber. Konsep tersebut merupakan hasil penelitian yang ditemukan oleh Gultom, Farid, Lestari, Lahallo dan Akbar (Gultom dkk, 2020). Instrumen SWCS memiliki 6 indikator yang dijadikan penilaian untuk mengukur keamanan siber di suatu instansi yang dapat dilihat pada Tabel 2.2.

Tabel 2.2. Indikator pada Instrumen SWCS (Gultom, 2019)

No.	Indikator
1.	Brainware
2.	Hardware
3.	Software
4.	Infrastructureware
5.	Firmware
6.	Budgetware

Six-Ware Cyber Security (SWCS) merupakan sebuah konsep komprehensif untuk solusi keamanan siber dalam meningkatkan ketahanan keamanan jaringan negara dari berbagai ancaman, serangan dan kerentanan

serta dalam melawan aktivitas ekstremisme kekerasan di dunia maya. SWCS dapat dikatakan sebagai strategi keamanan tingkat operasional yang memungkinkan untuk mengetahui tindakan paling efisien dan efektif yang dapat mengarah pada keberhasilan operasi keamanan siber. Ide dibalik konsep SWCS ini terinspirasi dari platform keamanan siber NIST versi 1.0. Jadi, konsep ini akan mengelaborasikan kerangka keamanan siber NIST menjadi lebih praktis dalam tingkat operasionalnya. Konsep SWCS menyumbangkan pemikiran bersama dalam memahami, mengelola dan mengungkapkan risiko keamanan jaringan baik secara internal maupun eksternal (Gultom dkk, 2018). Terdapat 6 aspek utama dalam Six-Ware Cyber Security, yaitu :

a. Brainware atau dapat disebut faktor manusia. Ini merupakan aspek utama dalam lingkungan keamanan jaringan. Variabel ini menjadi faktor paling penting pada konsep SWF. Pada perspektif keamanan jaringan, manusia merupakan mata rantai terlemah dalam lingkungan keamanan informasi. Faktor manusia memainkan peranan dominan untuk meningkatkan atau mengganggu semua upaya keamanan informasi yang ada dalam suatu organisasi. Oleh karena itu, organisasi harus memiliki fungsi atau jabatan yang berkaitan dengan keamanan informasi.
b. Hardware, memainkan peran dominan yang menangani ancaman, serangan dan kerentanan. CISO memiliki tanggung jawab untuk mengajari semua karyawan tingkat mengenai bagaimana menggunakan dan memperlakukan hardware organisasi dengan aman dan bijaksana. Hal ini bertujuan untuk berlindung dari hacker karena seorang hacker yang sudah professional tidak hanya mengandalkan teknik tertentu, tetapi masih dikombinasikan dengan serangan konvensional seperti rekayasa sosial. Kombinasi penilaian risiko internal dan analisis ancaman sangat diperlukan, contohnya dengan

mengontrol akses individu ke dalam fasilitas organisasi, mengunci sistem dan menghapus CD-ROM atau USB thumb drive yang tidak perlu, memantau dan melindungi parimeter keamanan fasilitas organisasi dan sebagainya.

c. Software, berkaitan dengan pemanfaatan perangkat lunak keamanan aplikasi yang digunakan sehari-hari di kantor seperti email, website dan media sosial. Kesadaran akan keamanan yang tinggi sangat diperlukan karena hacker professional akan selalu mencoba untuk menginfeksi atau menyuntikan email berbahaya atau mengundang untuk mengunjungi situs web yang terinfeksi malware.
d. Infrastructureware, faktor ini memiliki peranan penting dalam memfasilitasi infrastruktur jaringan organisasi yang aman, contohnya memantau jaringan dari berbagai ancaman dan serangan. Saat ini, sebagian besar perusahaan sangat bergantung pada akses internet. Di sisi lain, tidak semua karyawan memiliki tingkat pemahaman yang baik mengenai risiko keamanan yang mereka hadapi sehingga kondisi ini membuat infrastruktur jaringan organisasi menjadi lebih rentan.
e. Firmware, termasuk dokumentasi dan kebijakan keamanan organisasi, prosedur operasi standar (SOP), rencana kelangsungan bisnis (BCP), kerangka kerja keamanan jaringan atau organisasi internasional untuk standarisasi (ISO).
f. Budgetware, faktor ini mempunyai peranan penting dan strategis dalam memfasilitasi implementasi variabel 5 ware sebelumnya. Hal ini karena organisasi didesak untuk menyediakan uang yang cukup besar atau anggaran yang cukup untuk membeli, misalnya alat aplikasi keamanan jaringan, sistem patch, lisensi perangkat lunak, pelatihan dan pendidikan, serta program sertifikasi. Perlunya untuk manajemen tingkat atas harus menempatkan faktor ini sebagai prioritas dalam membangun kesadaran keamanan informasi. Mengalokasikan

anggaran keamanan informasi yang cukup dapat melindungi seluruh sistem jaringan. Jika tidak, maka akan berdampak pada kerugian finansial yang signifikan.

2.1.4 Portabilitas Instrumen Pengukuran

Kata “portabilitas” dapat diartikan sebagai kemampuan dari sebuah *software* untuk ditransfer dari satu sistem ke sistem yang lain. Defenisi lain dari portabilitas adalah bagaimana suatu elemen tertentu dapat disesuaikan dengan lingkungan baru. Jika sejumlah elemen cukup sesuai dan mudah diadaptasi, maka model tersebut dapat dikatakan sebagai portabel dengan syarat hasil implementasinya berhasil. Dalam lingkungan industri telematika, portabilitas masih berhubungan dengan cara adaptasi suatu *software* atau instrumen yang akan ditransfer dari lingkungan yang berbeda. Portabilitas merupakan usaha yang diperlukan untuk memindahkan suatu program dari sistem *software* satu dengan *software* lainnya (McCall, 1977).

Pada penelitian Terenciani (2016) menjelaskan bahwa pada ISO 25000 mendefenisikan portabilitas sebagai tingkat efektivitas dan efisiensi dimana sistem, produk serta komponen dapat dipindahkan dari satu *hardware, software* atau lingkungan operasional atau pengguna yang satu ke yang lainnya. Portabilitas memilik beberapa karakteristik yang perlu diperhatikan, yaitu :

a. Adaptabilitas : didefenisikan sebagai sejauh mana sistem atau instrumen diadaptasi pada *hardware, software,* dan lingkungan operasional yang berbeda-beda secara efektif dan efisien.
b. Installability : kemampuan dari *software* untuk diinstall pada lingkungan yang berbeda-beda.
c. Replaceability : didefenisikan sebagai sejauh mana suatu produk bisa menggantikan produk *software* yang lain dengan tujuan dan lingkungan yang sama.

Portabilitas instrumen pengukuran merupakan kemudahan suatu instrumen dapat digunakan untuk menggukur dari satu objek ke objek lainnya. Hal yang perlu diperhatikan dalam menentukan portabilitas suatu instrumen pengukuran, yaitu analisis statistiknya, kemudahan baca dan outlier yang muncul. Tiga faktor tersebut akan mempengaruhi portabilitas suatu instrumen pengukuran.

2.1.5 Analisis Varian

Analisis varian (ANOVA) adalah alat keputusan untuk mendeteksi variasi parameter proses. Ini merupakan teknik statistik yang digunakan untuk mengetahui tingkat faktor yang optimal dalam verifikasi parameter desain optimal melalui percobaan konfirmasi. ANOVA menentukan apakah terdapat perbedaan statistik di antara dua kelompok atau lebih, tetapi tidak menentukan kelompok mana yang memiliki perbedaan secara signifikan (Lynne, 2021). Pernyataan tersebut menjelaskan apabila tes ini signifikan, maka menunjukkan cara setidaknya satu pasangan berbeda, tetapi tidak mengetahui pasangan yang mana. Hal tersebut membutuhkan tes tambahan (Mishra dkk, 2019). ANOVA merupakan proses sistematis dengan tujuan mengidentifikasi dan menjelaskan varians atau penyimpangan hasil yang sebenarnya dari hasil yang diharapkan. ANOVA digunakan sebagai alat analisis dalam pengujian hipotesis penelitian yang mana apakah terdapat perbedaan rerata kelompok. Analisis varians juga digunakan dalam eksperimen yang mana diberikan beberapa perlakuan berbeda yang tujuannya untuk menguji apakah terdapat perbedaan yang bermakna pada perlakuan tersebut. ANOVA akan menghasilkan output berupa F hitung. Jika nilai F hitung tersebut lebih besar dibandingkan dengan F tabel, maka menunjukkan bahwa menerima Ho dan menolak Ha. Hal tersebut menjelaskan bahwa tidak terdapat perbedaan rerata pada semua kelompok.

Pada ANOVA satu arah, variabel independen bersifat kategoris seperti sebelum dan sesudah pelaksanaan intervensi yang berbeda, seperti intervensi untuk mengurangi kesalahan pengobatan dan variabel terikat yang berkelanjutan seperti prevalensi kesalahan pengobatan. ANOVA bisa lebih kompleks dari ini dengan beberapa faktor independen yang dikenal dengan ANOVA dua arah (Larson, 2008). ANOVA satu arah mempunyai bentuk kriteria data, yaitu (Muhid, 2019):

- Data harus bersifat homogen dan berdistribusi normal.
- Data yang digunakan harus dalam bentuk kategori dan variabel dependen harus data yang bersifat kuantitatif seperti interval atau rasio.
- Sampel tidak memiliki hubungan antar satu dengan lainnya.

2.1.6 Kemudahan Baca Instrumen

Salah satu objek yang diukur dalam analisis portabilitas instrumen adalah kemudahan baca responden pada kuesioner tersebut. Analisis kemudahan baca tersebut dapat menggunakan metode *flesch reading ease*. Formula *flesch reading ease* merupakan pendekatan sederhana untuk menilai tingkat kelas pembaca. Ini juga salah satu dari sedikit ukuran akurat yang dapat diandalkan tanpa terlalu banyak pengawasan. Metode tersebut sudah digunakan sejak lama untuk menganalisis kemudahan baca dari sebuah buku atau majalah. Pada penelitian Eleyan (2020) menggunakan metode ini untuk meningkatkan keterbacaan komentar perangkat lunak. Peneliti Firdaus (2020) menggunakan metode ini untuk menganalisis tingkat kebacaan teks bacaan buku pelajaran bahasa inggris bagi siswa SMA kelas 12. Menurut Richards (1992), formula *flesch reading ease* merupakan rumus keterbacaan yang mengukur seberapa mudah bahan tertulis dapat dibaca dan dipahami. Skor pada *flesch reading ease* yaitu 0 hingga 100. Ini menghitungnya menggunakan rata-rata panjang kalimat dan jumlah rata-rata

suku kata per kalimat. Semakin tinggi skor anda, semakin mudah dibaca konten tersebut. Kategori skor tersebut dapat dilihat pada Tabel 2.1.

Tabel 2.3. Skor Pada *Flesch Reading Ease* (DuBay, 2006)

Skor *Flesch Reading*	Tingkat Kesulitan	Level Kelas
90-100	Sangat Mudah	5
80-90	Mudah	6
70-80	Cukup Mudah	7
60-70	Biasa	8-9
50-60	Cukup Susah	10-12
30-50	Susah	Universitas
< 30	Sangat Susah	Lulusan Universitas

2.1.7 Analisis Outlier

Outlier adalah titik data yang secara signifikan berbeda dari data yang tersisa. Outlier disebut sebagai abnormal, sumbang, penyimpangan atau anomaly dalam data mining dan literatur statistik. Dalam sebagian besar aplikasi, data yang dibuat oleh satu atau lebih proses pembangkitan yang dapat mencerminkan aktivitas dalam sistem atau pengamatan yang dikumpulkan tentang entitas. Ketika proses pembangkit berperilaku tidak biasa, itu memunculkan outlier. Oleh karena itu, outlier sering berisi informasi yang berguna mengenai karakteristik abnormal dari sistem dan entitas yang berdampak pada proses pembuatan data. Awalnya, pendeteksian *outlier* dilakukan untuk pembersihan data seperti menghapus outlier dari kumpulan data sehingga model statistik parametrik dapat menyesuaikan data pelatihan dengan lebih lancar. Tetapi, saat ini pendeteksian *outlier* sering mewakili informasi yang menarik dan kritis, misalnya serangan dunia maya dalam jaringan, kesalahan mekanis yang disebabkan oleh peralatan industri yang

rusak dan sebagainya (Boukerche et al, 2020). Dengan mengidentifikasi *outlier*, peneliti dapat memperoleh pengetahuan penting yang membantu dalam membuat keputusan yang lebih baik tentang data. Defenisi lain mengenai *outlier* yaitu informasi yang dapat ditindaklanjuti secara signifikan dalam berbagai aplikasi (Wang et al, 2019).

Menurut Hawkins (1980) menyatakan bahwa outlier merupakan pengamatan yang sangat menyimpang dari pengamatan lain sehingga menimbulkan kecurigaan bahwa hal itu dihasilkan oleh mekanisme yang berbeda. Interpretabilitas model deteksi outlier sangat penting dari perspektif analis. Seringkali diinginkan untuk menentukan mengapa titik data tertentu harus dianggap sebagai outlier karena memberikan petunjuk lebih lanjut kepada analis mengenai diagnosis yang diperlukan dalam skenario khusus. Proses ini juga disebut sebagai penemuan pengetahuan intensif mengenai outlier atau deteksi dan deskripsi outlier (Aggarwal, 2017). Banyak peneliti telah mencoba menjawab pertanyaan tentang bagaimana mendeteksi *outlier*. Fitur-fitur penting yang perlu dipertimbangkan dan pengujian yang perlu dilakukan untuk mengidentifikasi *outlier* adalah pertanyaan yang sama pentingnya.

2.2 Hasil Penelitian Terdahulu

Sebelum penelitian tesis ini, beberapa peneliti terdahulu telah melakukan penelitian-penelitian yang menjadi sumber referensi dalam penulisan tesis ini. Pada penelitian yang penulis buat, terdapat beberapa perbedaan penelitian yang akan dilakukan dengan yang sudah peneliti lain laksanakan seperti variabel yang digunakan, penggunaan metode, serta teknik analisis. Pada dasarnya, penelitian terdahulu digunakan untuk melihat perkembangan penelitian dan mengetahui gap antar penelitian sehingga dapat menemukan keterbaharuan dari penelitian yang dilakukan. Berikut

adalah beberapa penelitian yang menjadi acuan dalam penelitian tesis ini seperti yang disajikan pada tabel 2.4.

Tabel 2.4. Hasil Penelitian Terdahulu

No	Nama Peneliti	Judul Penelitian	Pokok Bahasan	Perbedaan	Persamaan
1.	Nyoman Darmawan (2021)	Konsep Pembangunan Teknologi Cyber Security Berbasis Six-Ware Framework di Mako Lanal Palu	Menganalisis mengenai sistem militer di Mako Lanal Palu berbasis Six-Ware Framework menggunakan regresi linier.	Parameter yang digunakan, tujuan penelitian, metode penelitian	Objek penelitiannya menggunakan *Six-Ware Cyber Security*, Metode penelitian.
2.	Pamungkas Trishadiatmoko, Achmad Farid Wadjdi (2021)	Public Policy Implementation During Pandemic Covid: Modifying the Measurement Framework of The Electronic-Based Governance	Menentukan indeks portabilitas pengukuran SPBE di stasiun TVRI pusat dan TVRI daerah.	Tujuan penelitian, parameter yang digunakan, metode penelitian.	Objek penelitiannya menggunakan Sistem Pemerintahan Berbasis Elektronik, Metode

		System for Various Organization Levels of Indonesia Public Service Broadcasting (TVRI)			penelitian.
3.	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	Membahas mengenai menemukan rancangan sistem pertahanan siber yang efektif untuk melindungi infrastruktur dan sistem informasi pertahanan negara menggunakan cyber six-ware framework dan ANOVA.	Parameter yang digunakan, tujuan penelitian.	Objek Penelitian menggunakan *Six-Ware Cyber Security*, Analisis data.

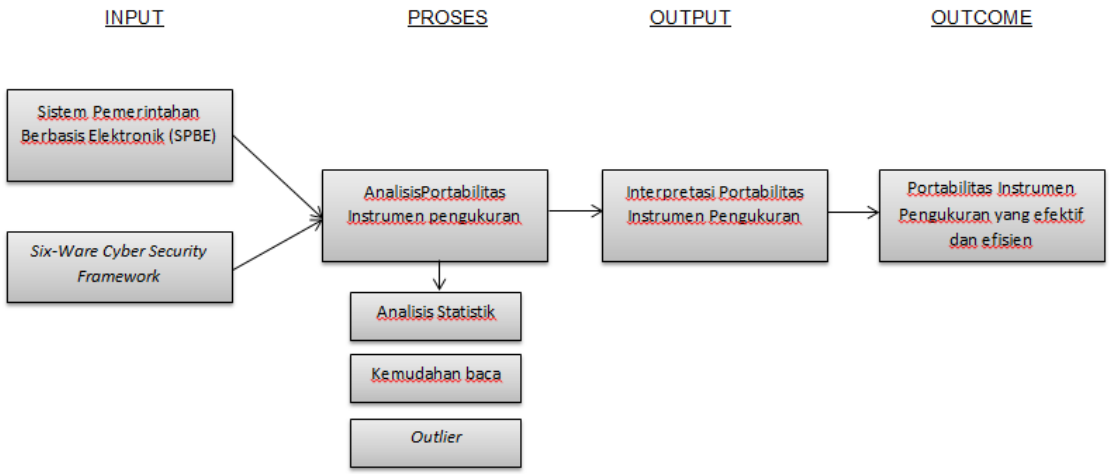
4.	Firdaus Anita (2020)	The Readability Level Of Reading Texts In English Textbook Entitled Bahasa Inggris For Senior High School Students Grade Xii	Menganalisis tingkat kebacaan buku pelajaran Bahasa Inggris kelas 12 menggunakan metode Flesch Reading Ease	Tujuan penelitian, Objek penelitian.	Analisis data menggunakan metode *flesch reading ease.*
5.	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	Membahas mengenai standar ASEAN Cyber Security Framework dalam rangka penanggulangan aktivitas cyber terrorism melalui internet serta memperkenalkan konsep awal Six-Ware Cyber Security.	Parameter yang digunakan, tujuan penelitian, metode penelitian	Objek Penelitian menggunakan *Six-Ware Cyber Security*.

6.	Pradita Maulidya Effendi, Tony Dwi Susanto (2019)	Test of Citizen' Physical and Cognitive on Indonesia E-Government Website Design	Membahas mengenai desain website yang bagus pada e-government menggunakan ANOVA.	Parameter yang digunakan, tujuan penelitian	Analisis data menggunakan ANOVA.
7.	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,	Evaluating the Interoperability of C4ISR System using Cyber Six-ware Framework	Membahas mengenai pengembangan interoperability pada C4ISR menggunakan Six-Ware Cyber Security dan regresi linier.	Parameter yang digunakan, tujuan penelitian, metode penelitian.	Objek Penelitian menggunakan *Six-Ware Cyber Security*.

	Gita Amperiawan (2021)				

2.3 Kerangka Pemikiran

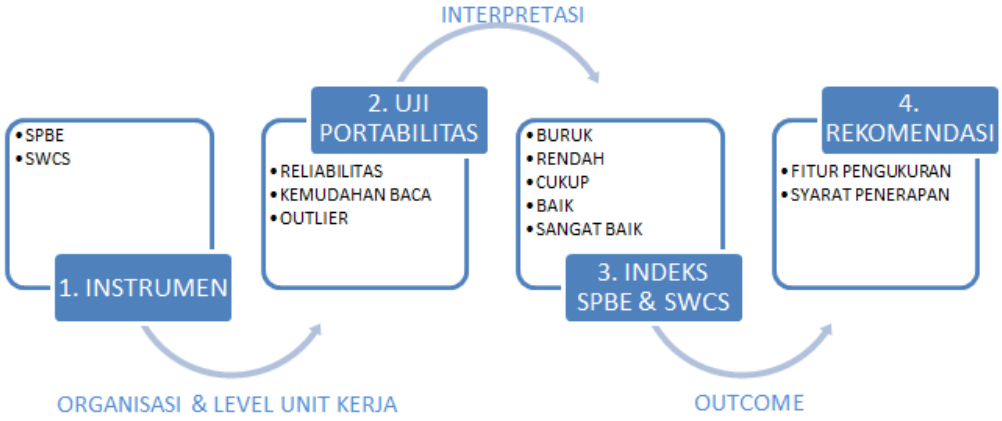
Permasalahan yang dibahas pada tesis ini dilatarbelakangi oleh fenomena perubahan sistem pengukuran objektif menjadi pengukuran subjektif dalam konteks implementasi digitalisasinya. Kedua instrument pengukuran tersebut yakni SPBE dan SWCS memerlukan analisis portabilitas untuk mendukung perubahan tersebut.



Gambar 2.1 Kerangka Umum Pemikiran

Sumber : diolah peneliti (2022)

Berdasarkan uraian diatas, kerangka pemikiran yang di ajukan dalam menguji portabilitas kedua kerangka pengukuran tersebut adalah sebagai berikut: Gambar 2.1 menjelaskan kerangka umum pemikiran pentingnya analisis portabilitas dari penelitian tesis ini. Instrumen SPBE dan SWCS merupakan objek yang akan diteliti. Selanjutnya, data yang diperoleh dari kuesioner instrumen tersebut dilakukan preparasi dan analisis data untuk melihat portabilitas dari kedua instrumen tersebut sehingga mendapatkan *outcome* berupa jawaban pertanyaan dari rumusan masalah yang disampaikan dalam Bab 1.



Gambar 2.2. Alur Pemikiran

Sumber: diolah peneliti (2022)

Gambar 2.2 merupakan bagaimana kerangka umum pemikiran tersebut dijabarkan dalam alur pemikiran untuk menjawab pertanyaan penelitian yakni berupa 1) Indeks Portabilitas kedua sistem pengukuran; 2) outcome dalam bentuk temuan fitur (yang membantu meningkatkan *security awareness*) dan syarat penerapan dari kedua sistem pengukuran (SPBE dan SWCS) untuk memperoleh pengukuran efektif dan efisien. Penjelasan lebih lanjut mengenai langkah-langkah penelitian sesuai kerangka dan alur pemikiran tersebut diuraikan dalam bab III.