BAB 2
TINJAUAN PUSTAKA

2.1 Landasan Teori

Bab 2 menjelaskan mengenai teori dan konsep yang digunakan peniliti saat melakukan penelitian. Teori dan konsep memiliki keterkaitan dengan permasalahan penelitian pada faktor-faktor kendala dalam membangun sistem siber di Pusat Pertahanan Siber di Kementerian Pertahanan Republik Indonesia. Teori yang dipakai dimaksudkan guna membimbing dan memahami pada masalah yang terpaut dengan pokok bahasan. Ada empat teoir yang dipakai, seperti: *grounded theory, middle theory* dan *apply theory*. *Grounded theory* yang dipakai adalah teori ilmu pertahanan. *Apply theory* yang dipakai adalah teori *sixware network security framework* (SWNSF*)*. Selain menyuguhkan teori, pada Bab 2 ini juga menyuguhkan beberapa penelitian sebelumnya yang memandingkan dengan penelitian ini.

2.1.1 Teori Ilmu Pertahanan

Makmur Supriyatno adalah seorang mantan anggota TNI angkatan darat yang memiliki pengaruh besar dan salah satu seorang pendiri di Universitas Pertahanan Republik Indonesia (Unhan). Brigadir Jenderal TNI (Purn) Makmur Supriyatno turut mengabdikan dirinya sejak unhan telah di bentuk sampai lima tahun dan purna tugasnya. Dalam dasar ilmu pertahanan yang di bahas pada buku “Tentang Ilmu Pertahanan”, Brigadir Jenderal TNI (Purn) Makmur Supriyatno memperdalam dengan pengalamannya ketika mengajar di Unhan, di beberapa lembaga pendidikan TNI dan perguruan tinggi lainnya.

Pertahanan negara sebagai upaya untuk dapat mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia dan keselamatan segenap bangsa dan negara terhadap adanya ancaman dan ganguan pada keutuhan suatu negara. Ini menjadikan sebuah tugas pokok dari negara yang dilakukan pemerintah untuk dapat

mempertahankan negara yang telah di tetapkan pada Undang-Undang Nomor 3 Tahun 2002 mengenai Pertahanan Negara (2002).

Menurut Makmur Supriyatno (2014) mengatakan ilmu pertahanan adalah cakrawala secara sistematis mengenai pilar-pilar perang atau peratahanan, adanya pengembangan yang sistematis, kemudian dilakukannya pemeriksaan atau evaluasi dari hasil analisis dan metode penyebaran yang tepat dalam pemahaman dari kemampuan yang dimiliki. Ilmu pertahanan harus dapat menangkal adanya ancaman yang berkembang dan dinamis. Ancaman tidak hanya dilakukan oleh negara atau organisasi, melainkan juga dapat berasal dari suatu negara yaitu "individu" yang melakukan kejahatan dan mengganggu terhadap suatu bangsa dan negara.

Dalam buku Tentang Ilmu Pertahanan karangan Makmur Supriyatno (2014) dikatakan adanya keterkaitan antara Ilmu militer, Ilmu dan Seni Perang dan Ilmu Pertahanan. Istilah kata strategi yang berasal dari Seni Militer (*Art of Military)*, bagaimana upaya dalam menerapkan keahlian dalam pengerahan kekuatan militer dalam suatu pertempuran atau peperangan. Seiring berjalannya waktu, berbagai kajian dan pengalaman terhadap peperangan pada masa lalu, kini telah berkembang menjadi Ilmu Militer (*Military Science*). Yang kemudian berlanjut menjadi sebuah Ilmu dan Seni Perang (*Science and Art of War*). Dalam penggunaan sumber daya militer tidak cukup dengan hanya keterampilan saja namun harus dikembangkan melalui teori dari hasil kajian.

Ilmu militer atau *military Science* dalam kajiannya mengenai cara, alat, bagaimana dan mengapa dapat memiliki keterkaitan satu sama lain terhadap masalah militer, seperti yang telah di definisikan: "*The study of the ways, means, as well as he hows and whys, of military affairs."* (Shafritz, 1989). Menurut Dame Rebbeca West (1892-1983) yang mana seorang jurnalis dan seorangg novelis yang berasal dari Inggris yang mengatakan, bahwa: sebelum adanya perang, militer hanya dijadikan sebuah ilmu pengetahuan, seperti astronomi, namun ketika perang militer seperti

“astrologi”. Ditulis, bahwa: “*Before war, military science seems a real science, like astronomous, but after a war it seems more like astrology*”. yang mana adanya perbedaan yang mendasar antara sebelum adanya perang dan setelah adanya perang.

Perang diartikan sebagai aksi kekerasan dari suatu negara kepada negara lain, melakukan kekejaman yang nantinya akan dirasakan oleh warga negara ketika sedang berlangsung. Seni perang merupakan sebuah bentuk pendekatan ilmiah terhadap aktivitas militer yang menggunakan kemampuan dan pembelajaran yang menghasilkan suatu pemecahan terhadap permasalahan militer. Menurut Henry Jomini (1836) dalam buku nya yang berjudul “*Precis de l’Art de Guerre”* yang menulis, bahwa: perang adalah “ensambel” yang memiliki arti yaitu bukan suatu ilmu menurut Hittle, J.D (1987). Menurut Makmur Supriyatno (2014) mengenai esensi dari perang juga dapat dilihat sebagai “*state violent”* atau bentuk dari konflik bersenjata yang dilakukan antara organisasi politik dengan usahanya untuk mendapatkan, mempertahankan dan dapat menambah kekuasaan politik dalam mencapai tujuan politik.

Dalam pola hidup yang semakin berkembang di dunia telah memberikan perubahan dengan adanya revolusi militer yang memiliki pengaruh yang sangat besar oleh perkembangan ilmu militer dan ilmu perang. Menurut Gongora dan Van Riekhoff yang menjelaskan mengenai *Revolution in Military of Art* (RMA) adanya sebuah proses transformasi dari organisasi militer, sistem persenjataan dengan menggunakan proses integrasi teknologi informasi secara potensial guna meningkatkan dan mengembangkan kekuatan militer konvensional demi kepentingan naisonal menurut Thierry and Harald von Riekhoff Gongora (2000). Dari sektor militer dapat memanfaatkan kecanggihan teknologi dengan cara melakukan perang informasi kepada suatu negara.

Teknologi militer yang dapat merubah substansi menjadi perkembangan revolusi militer pertama dan kedua, yang kemudian berubah menjadi teknologi informasi yang merupakan ciri-ciri dari RMA itu sendiri. Adanya perubahan antara teknologi militer dengan teknologi informasi yang dapat menciptakan ilmu pertahanan. Perang informasi pada saat ini semakin berkembang dan bentuk ancamannya pun semakin dinamis. Menurut Makmur Supriyatno (2014) mengatakan bahwa ilmu pertahanan harus mampu menjaga kedaulatan teritorial, sumber daya alam dan melindungi segenap bangsa dan negara, tetapi harus mampu menuju kekuatan dengan unsur *detterent strategy* atau strategi penangkalan agar dapat memberikan getaran kepada negara lain.

Sedangkan menurut Syarifudin Tippe (2016), mengatakan mengenai pertahanan adalah kebutuhan nasional yang sangat utama ketika kedaulatan negara telah mendapat adanya pengakuan. Pada ontologi ilmu pertahanan sebagai objek ilmu pertahanan yang dapat menunjukkan adanya perilaku negara untuk dapat mengembangkan, mengurangi atau bahkan meniadakan ancaman pada kedaulatan negara, menjaga negara yang memiliki hubungan dengan keamanan dalam tingkatan nasional demi tujuan penyelenggaraan pertahanan negara dan melestarikan keutuhan suatu wilayah dan keselamatan bangsa. Dari ilmu militer dan ilmu perang menghasilkan ilmu pertahanan.

Pada epistemologi menjadi ilmu yang lebih komprehensif yang dapat menjadi multidisiplin, interdisiplin dan transdisiplin. Dan sedangkan pada aksiologi adalah ilmu pertahanan yang dapat memberikan adanya kontribusi yang sangat penting pada pengembangan kebijakan pertahanan negara yang memberikan manfaat pada dunia internasional yang dapat menciptakan hubungan yang harmonis, damai dan dinamis dengan antar negara.

Menurut Miriam Budiardjo (2008), mengatakan pertahanan negara dapat tumbuh dan berkembang pada adanya sistem politik yang menyangkut dengan penyelenggaraan fungsi peratahanan negara pada kerangka sistem politik. Pengembangan ilmu pertahanan memiliki fokus pada penelitian pada teknologi melalui pengembangan studi ilmu-ilmu sosial.

2.1.2 Teori Strategi

Carl Von Clausewitz adalah seorang *theorist* yang berasal dari Prusia dan memiliki pengaruh pada dunia militer. Urusan negara kini berkembang menjadi jaringan yang saling ketergantungan dikarenakan dengan adanya kerjasama, persaingan yang semakin kompleks dan tekanan yang diberikan semakin meningkat pada negara yang secara efektif dengan menggunakan alat kenegaraan untuk dapat mencapai objek politik. Menurut Tri Legionosuko dan Marsono (2020) mengenai teori perang dan strategi yang telah di tulis dalam buku "*On War*" yang menyatakan bahwa strategi besar telah dibantu untuk dapat menyajikan kondisi politik.

Menurut Clausewitz (1943) mengenai strategi merupakan bentuk perang yang berkelanjutan dari politik yang tidak dapat dipisahkan dari trinitas sekunder, bangsa dan negara yang terdiri dari rakyat, militer dan pemerintah. Bangsa dan negara di karakteristikan pada keahlian yang dapat memanfaatkan materi dan energi dari rakyat dan dapat merubah menjadi aktivitas perang. Dari perang juga dapat menjadikan fasilitas hubungan politik yang di karakteristikan pada kekuatan militer guna mencapai tujuan politik.

Menurut Sofjan Assauri (2013) terdapat fungsi strategi, seperti:

a. Adanya komunikasi dari visi yang ingin dicapai.
b. Adanya hubungan antara kekuatan dan keunggulan organisasi dengan memanfaatkan peluang dari kondisi sekitarnya.
c. Memanfaatkan keberhasilan yang telah dicapai yang kemudian menganalisis adanya kesempatan baru untuk nantinya.
d. Menciptakan dan membangun potensi sumber-sumber daya yang lebih banyak.
e. Adanya sistem dan membimbing aktivitas organisasi yang mengarah ke masa depan. Menganalisis atau mengulas suatu kejadian yang baru dihadapi.

Unsur kekuatan yang dilakukan secara menyeluruh dan terarah dibawah kesatuan perintah atau komando yang menggabungkan adanya strategi dalam pertahanan yang menghasilkan suatu totalitas pertahanan negara. Menurut Buku Putih Pertahanan Republik Indonesia (2015) mengenai strategi pertahanan telah merangkum pada tujuan, sasaran, upaya dalam mencapai apa yang hendak ingin dituju dan sumber daya pertahanan guna membangun kekuatan dan kemampuan pertahanan negara yang efektif, tangguh dan berdaya tangkal yang tinggi.

Strategi Sistem pertahanan Indonesia telah menganut pada UU No. 3 Tahun 2002 (2002).tentang Pertahanan Negara pada pasal 1 Angka 1 UU Pertahanan Negara, yaitu: Segala upaya guna mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara.

Teori-teori yang dipakai oleh Clausewitz menitik beratkan pada aspek moral dan politik, adanya penggunaan konsep romantik dan konsep Hegelian dalam kondisi peperangan, adanya penekanan pada penjelasan mengenai bagaimana faktor-faktor yang saling berlawanan dapat saling berinteraksi satu sama lain dan mencatat adanya perkembangan baru dalam “kabut perang” yang tidak terduga dan dapat menghasilkan

keputusan yang cepat dan tepat dari para pemimpin atau komandan atas reaksi yang di dapatnya menurut Raymond Aron (1983).

Menurut Clausewitz (1943) ini menjadikan dasar *Grand strategy* yang terdapat adanya kompleks logis dari instrumen hubungan politik yang telah berorientasi pada strategis, kemudian terdiri dari data tata bahasa diplomasi, ekonomi dan perang. Konsepsi yang dipakai oleh Clausewitz untuk dapat menggambarkan strategi besar sebagai totalitas saran hubungan politik yang menawarkan satu cara untuk dapat mengintergrasikan satu sama lain antara alat kenegaraan kedalam satu pandangan dengan kebijakan negara dalam hubungan yang lebih tinggi.

Dalam dasar ilmu fisika modern yang membahas mengenai keadaan ilmu mekanik yang mana pusat gravitasi telah mewakili titik dimana gaya gravitasi bertemu dalam suatu objek. Untuk dapat menyerang pusat gravitasi diperlukan kekuatan yang cukup besar agar dapat menyebabkan kehilangan pada keseimbangan. Maka dari itu sistem siber dapat menjadikan strategi pushansiber sebagai pusat gravitasi untuk dapat mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara.

Oleh karena itu pusat gravitasi yang dipakai oleh Clausewitz adalah bukan sumber kekuatan melainkan faktor keseimbangan. Pusat gravitasi ditentukan oleh seluruh sistem (struktur) dari musuh, ketika dilihat bukan dari tingkat perang, melainkan untuk dapat mengalahkan musuh sepenuhnya dengan cara mencari dan menghancurkan lokasi dari pusat gravitasi pada perang. Perlu diketahui bahwa pihak lawan telah di persenjatai dengan senjata kimia, biologi, radiologi, nuklir dan bahan peledak yang memiliki daya ledak tinggi yang dapat beroperasi secara terdensentralisasi secara global yang perlu di perhatikan. Tingkat strategis, Clausewitz mengidentifikasi militer suatu negara sebagai salah satu pusat gravitasinya.

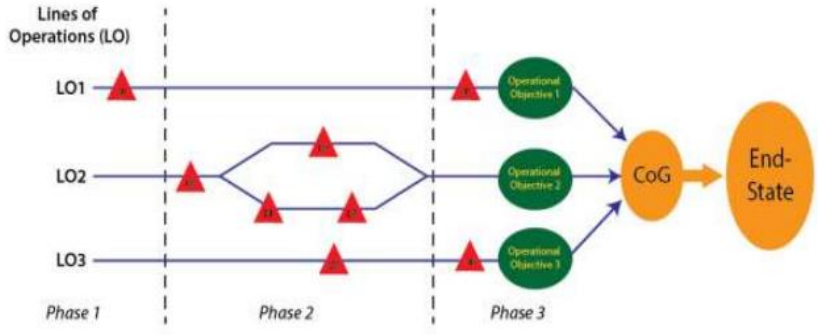
Sir Basil Henry Liddell Hart merupakan ahli teori militer yang merupakan seorang prajurit inggris dan merupakan sejarahwan militer pada abad ke-20. Liddell Hart juga menjelaskan mengenai arti dari strategi. Menurut Liddell Hart (1967), mengatakan strategi menjadi seni yang dapat mendistribusikan dan diterapkan pada sarana militer untuk dapat mencapai tujuan akhir kebijakan. Dari penggunaan dan pendistribusian strategi dapat menjadikan *ways,* kemudian pada sarana militer dapat menjadikan *means*¸dan sedangkan untuk mewujudkan tujuan dari akhir kebijakan dapat menjadikan *ends.* Dapat disimpulkan bahwa strategi dapat menjadikan penentuan dari tujuan (*ends*) yang kemudian menciptakan cara untuk dapat di tempuh (*ways*) yang nantinya dapat menentukan sarana dan prasarana nya (*means*) guna mencapai tujuan.

Liddle Hart juga lebih menekankan pada gerakan, fleksibel dan adanya kejutan yang dikarenakan dari sebagian kampanye militer, dislokasi keseimbangan psikologis dan fisik musuh menjadikan awal dari kemenangan. Dari dislokasi ini dapat menjadikan strategi.

Tingkat strategis pada pusat gravitasi dapat mencakup kekuatan militer, aliansi, kemauan nasional atau dukungan publik, serangkaian dari kemampuan atau fungsi penting, atau strategi nasional. Maka dari itu pihak Pusat Pertahanan Siber selalu berusaha untuk dapat membangun sistem siber yang nantinya akan digunakan pada kondisi apapun dan menjadikan bentuk dari antisipasi terhadap adanya ancaman siber di Indonesia.

Jika konsepnya tidak dapat didefinisikan dengan jelas atau dipahami dengan baik, pekerjaan yang dilakukan dalam upaya mengidentifikasi pusat gravitasi musuh adalah upaya akan menjadi sia-sia dan tidak menawarkan utilitas dalam desain kampanye. Meskipun desain kampanye menjadikan pusat gravitasi sebagai pusat prosesnya, ada banyak penekanan yang telah ditempatkan pada pengidentifikasikan pusat gravitasi tanpa mempertimbangkan jenis operasi yang sedang dipertimbangkan (konvensional atau lainnya) dan pada tingkat apa (taktis, operasional) atau strategis).

Sebagaimana dinyatakan dalam Jurnal publikasi Kanada lainnya, Doktrin dari Kanada yang lebih mengarahkan pada stafnya untuk dapat mencari beberapa pusat gravitasi di tingkat operasional. Menurut *Departement of National Defence* (2008) mengenai tanah Operasi menguraikan konsep untuk memasukkan pusat gravitasi "di setiap tingkat komando, dan musuh mungkin memiliki lebih dari satu Pusat gravitasi. Pusat gravitasi akan ada di mana pun kekuatan paling banyak terkonsentrasi dan di mana ada kohesi yang signifikan.



Gambar 2. 1 Desain Operasional. Mandaher (2014)

Pada gambar di atas ini mengenai garis operasi mewakili tindakan kekuatan yang diperlukan, atau kritis jalan seperti yang dinyatakan oleh publikasi desain kampanye yang mana untuk mencapai tujuan operasional. Ketika tujuan operasional tercapai dan pusat gravitasi akan dikalahkan, maka semua akan mengarah pada keadaan akhir. Terdapat cara lain untuk melihat grafik ini adalah dengan mempertimbangkan hambatan utama antara upaya pasukan persahabatan dan keadaan akhir yang mereka inginkan. Kendala utama adalah pusat gravitasi. Jika pusat gravitasi tidak dikalahkan, keadaan akhir tidak dapat dihubungi. Sangat mudah untuk melihat daya tarik konsep pusat gravitasi untuk desain kampanye. Ini dapat menjadikan sebuah pendekatan sistemik untuk mendefinisikan konsep operasional yang melalui ketekunan, upaya staf gabungan, menghasilkan desain kampanye dengan garis operasi, poin yang menentukan, dan tujuan operasional untuk mencapai keadaan akhir. Kelemahan dalam doktrin ini adalah pusatnya konsep pusat gravitasi.

2.1.3 Teori *Sixware Network Security Framework* (SWNSF)

Kolonel Sus Dr. Ir Rudy AG Gultom adalah seorang dosen tetap di Universitas pertahanan Republik Indonesia. Beliau memberikan pengaruh terhadap dunia siber di sektor militer. Beliau menciptakan sebuah teori *Sixware Network Security Framework* (SWNSF) dalam menghadapi ancaman siber. Teori SWNSF dapat di terapkan pada pembangunan system siber untuk dapat menjaga dan melindungi jaringan komputer di Indonesia.

Teori SWNSF menjadi kerangka dan strategi untuk meningkatkan keamanan pada jaringan komputer sistem informasi pertahanan atau militer dari adanya bentuk serangan dan ancaman yang dapat mengganggu, merusak dan menhancurkan sistem siber pada pertahanan Indonesia. SWNSF telah berkontribusi secara efektif dalam melindungi jaringan komputerisasi.

Teori SWNSF mencoba untuk mengembangkan kerangka keamanan jaringan pada NIST agar dapat lebih praktis dan efisien dalam tingkat operasional dan kerangka keamanan nya dapat ditemukan pada sistem ekstraksi data *web mashup* menurut Rudy AG Gultom (2011). SWNSF telah memberikan kesadaran terhadap keamanan lingkungan di organisasi untuk dapat mengamati bahaya internal atau eksternal dan menganalisis kebijakan terhadap adanya ancaman. Serangan siber memiliki tujuan dalam menguasai, memodifikasi, memasuki, merusak, mencuri dan menghancurkan dan melumpuhkan sistem aset infromasi yang dapat mengancam keamanan nasional, seperti adanya perang siber dan gangguan siber dalam Pedoman Pertahanan Siber, Kementerian Pertahanan Republik Indonesia (2014).

Apabila ingin membangun kedaualatan siber nasional yang kuat, perlunya adanya perhatian pada bentuk ancaman di dunia siber yang sering terjadi, seperti: serangan *Advanced Persistent Threats (APT) Denial of Service (Dos)* dan *Distributed Denial of Service (DDoS)* yang melakukan *verloading* pada kapasitas sistem dan dapat mencegah para pengguna sah dalam menggunakan dan mengakses sistem atau sumber daya yang sudah masuk pada penargetan. Kemudian adanya serangan *Defacement* yang dilakukan dengan melakukan modifikasi atau penggantian pada halaman web dari korban yang kemudian isi dari halaman web tersebut dapat berubah sesuai dengan perubahan yang dirubah oleh si penyerang. Lalu adanya serangan *Malware* yang telah terjadi dimana-mana dan dapat memberikan pengaruh pada semua orang yang terlibat pada tiap kegiatan. *Malware* juga merupakan suatu program atau kode yang berbahaya untuk dapat mengganggu pada operasi normal dari sebuah sistem komputer. Dari serangan *Malware* sendiri dapat memberikan keuntungan finansial dalam Pedoman Pertahanan Siber, Kementerian Pertahanan Republik Indonesia (2014). Dari teknik bentuk serangan pada dunia siber masuk pada dimensi logika yang dapat memberikan dampak pada kerugian ekonomi dan reputasi.

Kemudian menurut BSSN terdapatnya bentuk ancaman dan serangan dari dimensi fisik, seperti: adanya pencurian, bom dan lain-lain yang dapat memberikan dampak pada kematian, korban luka, kerugian ekonomi dan reputasi. Sedangakan bentuk ancaman pada konten Sosial-Budaya, seperti: video porno, konten dewasa dan negatif, *fake news, hoax* dan lain-lain yang dapat memberikan dampak reputasi, kehilangan identitas dan karakter nasional, kerugian ekonomi, kehilangan kedaulatan dan kehormatan dan kehilangan generasi masa depan menurut Asep Chaerudin (n.d.).

Pada semua tingkatan tinggi maupun rendah harus dapat terlibat dan berkontribusi dalam pengimplementasian dari teori SWNSF. Ketika kita melihat teori SWNSF telah mengadopsi dari keamanan jaringan NIST versi 1.0. Dalam SWNSF terdapat 6 unsur utama, yaitu: faktor manusia (*Brainware*), perangkat keras (*Hardware),* perangkat lunak (*software),* perangkat infrastruktur (*infrastructure), firmware* dan anggaran (*budgeting).*

Faktor manusia yang terlibat pada teori SWNSF yang berperang penting dalam peran dalam pelaksanaan dan mengoperasikan pada sistem komputer. Manusia dapat dikatakan sebagai *Brainware* yang juga memiliki hubungan dengan komputasi. Menurut Aulya Triya Larasati (n.d) *Brainware* termasuk dari perangkat yang memiliki intelektual dalam memakai dan dan dapat menjelajahi keahlian dari *hardware* (perangkat keras) dan *software* (perangkat lunak). Manusia yang menjadi suatu elemen sistem komputer *brainware* yang dapat melakukan aktivitas pada sistem siber guna mempersiapkan atau mengolah konsep yang menghasilkan suatu data yang dikerjakan oleh komputer.

Sumber daya manusia mulai di kembangkan dengan melalui pendidikan dan latihan di dalam dan di luar negeri pada personel TNI guna menghadapi ancaman siber yang dapat mengancam kedaulatan negera. Dengan adanya perang memberikan kondisi yang mekasa pada TNI agar memiliki *nonwar skills* menurut Barry Buzan (1991). Hubungan antara sipil dan militer juga diperlukan dengan melakukan pelatihan yang terintegrasi, memahami mengenai pola dari operasi, adanya instansi dari nonmiliter juga dapat memberikan dukungan dalam bentuk personel dalam Media Peneliti (n.d.).

TNI telah melakukan kerjasama dengan Hawaian National Guard (HING) dengan latihan bersama dalam keamanan siber dan sistem teknologi dalam Pontas (2019). Apabila dari faktor manusia nya dapat terlaksana dengan baik, maka terbentuklah kemampuan dalam menggunakan atau mengaplikasikan sistem siber dalam menjaga pertahanan Indonesia.

Menurut William D Duncan (2017) mengenai adanya faktor yang kedua dari teori SWNSF mengenai perangkat keras (*Hardware)* terdiri dari semua komponen elektronik dan perangkat elektromekanis yang dapat membentuk entitas kesatuan sistem *Personal Computer* (PC) yang nampak secara fisik menurut. Perangkat keras yang mumpuni sangat di perlukan pada sistem siber agar dapat menjadi bagian pendukung dari aktivitas pertahanan siber.

Menurut Aulya Triya Larasati (2021) mengenai faktor yang ketiga dari teori SWNSF tentang perangkat lunak (*Software*) merupakan program yang memiliki kegunaan sebagai sarana terjadinya interaksi yang dapat menjembatani antara sumber daya manusia (*brainware*) dengan perangkat keras. Diperlukan perangkat lunak khusus pada sistem siber agar dapat menerjemahkan perintah yang diberikan oleh *brainware* yang nantinya diteruskan dan diproses oleh perangkat keras.

Menurut R Kelly Rainer and Efraim Turban (2008) mengenai faktor yang keempat dari teori SWNSF tentang perangkat infrastruktur (*infrastructure)* menurut Turban, Rainer, & Potter mengenai perangkat infrastruktur (*infrastructure)* merupakan bentuk dari fasilitas fisik dengan adanya komponen dan layananan teknologi informasi yang dapat memanajemen teknologi informasi yang mendukung kegiatan keseleuruhan. Perangkat infrastruktur menjadikan suatu penunjangan utama dari teknologi untuk sistem siber agar dapat berjalan dan terselenggaranya proses infromasi dengan terarah dan cepat. Pada perangkat infrastruktur juga dilengkapi dengan layanan pada perusahaan

atau badan yang nantinya dialokasikan oleh manajemen yang terdiri kemampuan manusia di penggunaan sistem siber.

Faktor yang kelima dari teori SWNSF adalah *firmware. Firmaware* merupakan perangkat kecil yang hanya berada pada dalam *software* yang nantinya dapat membantu *hardware* bekerja atau beroperasi yang sesuai diinginkan. Menurut Badan Siber dan Sandi Negara (2021) mengenai kumpulan instruksi atau arahan nantinya dapat dimanfaatkan dalam melakukan penyaringan, pengaturan dan pengontrolan data yang diizinkan pada perangkat lunak. *Firmware* harus melakukan update agar sistem pada siber tidak mengalami kerusakan. *Firmware* yang dimiliki oleh Badan Siber dan Sandi Negara adalah melakukan meng-*update firmware* dari *Secure Mobile Access* (SMA) ke seri 10.2.0.5-29sv untuk dapat melakukan konfigurasi ulang pada *password* pada setiap pengguna yang telah masuk ke perangakat, mengaktifkan *multifactor authentication* dan *Web Application Firewall* untuk mengurangi kerentanan dari SNWLID-2021-0001 pada perangkat SMA 100 seri 10.x.

Pada *Firmware* terdapat Peta Okupasi Keamanan Siber yang telah dibuat oleh Badan Siber dan Sandi Negara. Dalam pembuatan Peta Okupasi Keamanan Siber ini menjelaskan penetapan *firmware* yang dapat memperkaya dan menambah jumlah okupasi yang ada. Dibawah ini terdapat gambar Peta Okupasi Nasional Keamanan Siber yang telah di buat oleh pihak Bidan Siber dan Sandi Negara:

Gambar 2. 2 Peta Okupasi Nasional Keamanan Nasional (Negara B. S., 2019)

Sumber: Badan Siber dan Sandi Negara

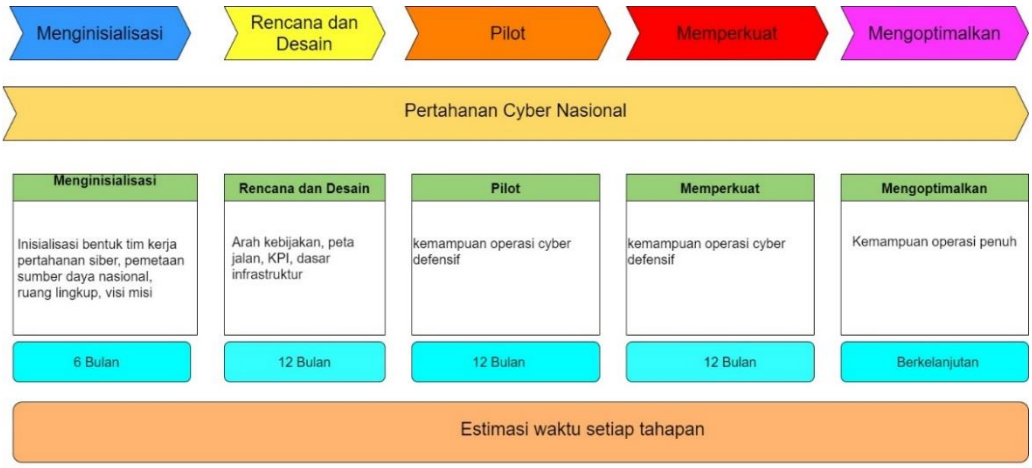
Pemerintah fokus dalam membangun sistem siber pada anggaran (*Budgeting*) yang telah sesuai dalam 6 faktor dari teori SWNSF yang dikemukakan oleh Rudy AG Gultom. Penekanan dalam strategi pertahanan siber Indonesia di Pushansiber yang memerlukan anggaran agar dapat terlaksana dengan baik. Pada instansi Kementerian Pertahanan Republik Indonesia telah menyiapkan dana sebesar Rp. 1.973.733.000,00 untuk dapat membeli dan membangun sistem siber seperti alat pemantau (sensor, router *firewall*) dan jaringan sistem pertahanan siber pada tannggal 26 Februari 2021 dalam LPSE Kemhan (2021) dan Sedangkan dari pihak BSSN telah menyediakan anggaran tahunan 2021 guna kebutuhan seharusnya sebesar Rp 4,4 Triliun dengan rincian Rp 3,2 Triliun dalam Badan Siber dan Sandi Negara (2020)

Menurut Marsda TNI Asep Chaerudin, mengatakan peran industri sangat penting dalam meningkatkan kemampuan dasar siber seperti: (n.d.)

a. Peralatan (*device*): gadget dan *IoT (Internet of Thing)*
b. Piranti Lunak (*software*): fintech, aplikasi integratif, anti virus/ malware
c. Jaringan: satelit dan serat optik

Kementerian Pertahanan telah membuat kebijakan dalam pertahanan siber agar dapat menciptakan kekuatan, seperti adanya peta jalan strategi nasional pertahanan siber, seperti:

Tabel 2. 1 Peta Jalan Strategi Siber Nasional



Sumber: diolah peneliti 2021

2.1.4 Teori Keamanan Sistem

Sistem siber dapat dijalankan dikarenakan adanya jaringan komputer. Jaringan komputer yang sistemnya terdiri dari komputer dan perangkat jaringan lain yang dapat bekerja sama satu dengan yang lain agar dapat mencapai tujuan yang diinginkan dalam Kominfo (2020). Dengan adanya jaringan komputer, sistem siber dapat memberikan dan bertukar informasi data dari komputer satu dengan yang lainnya. Informasi data tersebut dapat yang dilakukan oleh jaringan komputer, berupa: suara, video, gambar dan teks menurut Syafnidawati (2020). Menurut Iwan Sofana (2013) didalam jaringan komputer terdapat tiga jenis, seperti: *Local Area Network* (LAN), *Metropolitan Area Network* (MAN), *Wide Area Netwo5rk* (WAN) dan *Personal Are Network* (PAN):

a. *Local Area Network* (LAN)

   LAN adalah jaringan komputer hanya dapat mencakup wilayah kecil, seperti: jaringan gedung, kantor, sekolah dan kampus. LAN sendiri berbasis teknologi *IEEE* 802.3 Dari *Ethernet* telah menggunakan perangkat *switch*, dengan memiliki kecepatan transfer data mencapai 10, 100, 1000 Mbps. Teknologi *Ethernet* pada saaat ini teknologi 802. 11b yang biasa dikenal dengan *WiFi.*

b. *Metropolitan Area Network* (MAN)

   MAN hampir sama dengan LAN. Namun yang berbeda hanya pada area nya yang lebih besar dan komputer yang di hubungkan pada jaringan ini dapat mencakup lebih banyak dibandingkan dengan LAN. Jaringan MAN sendiri dapat mencakup seukuran kota atau gabungan dari LAN yang telah dihubungkan menjadi jaringan yang lebih besar. Jaringan MAN juga dapat digunakan oleh pihak sekolah dan kampus yang kemudian dapat diimplementasikan pada *wire* dan *wireless network.*

c. *Wide Area Network* (WAN)

   WAN merupakan jaringan komputer yang cakupan areanya besar dan digunakan untuk menghubungkan jaringan lokal satu dengan yang lain yang nantinya dapat memberikan manfaat kepada manusia dalam berkomunikasi yang menggunakan komputer.

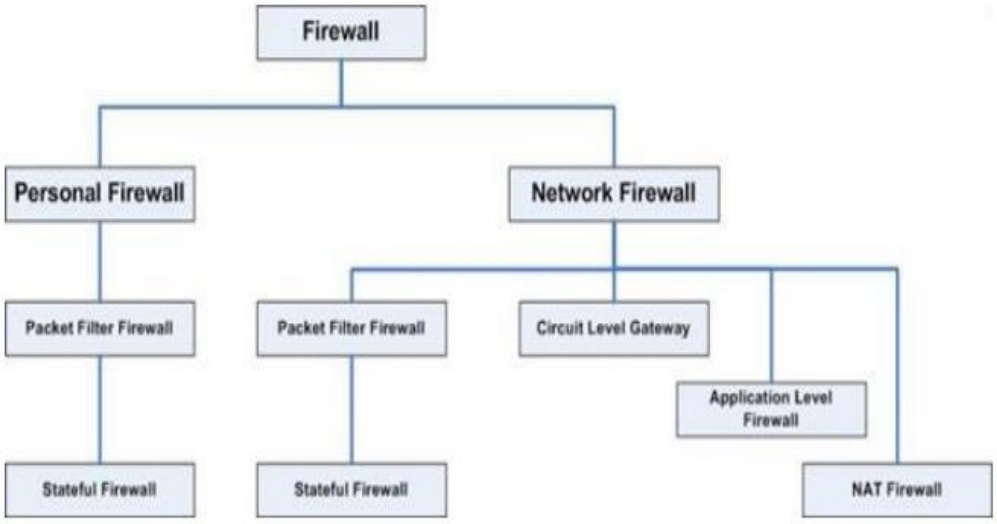
d. *Personal Are Network* (PAN).

   Personal Are Network (PAN) adalah suatu jaringan komputer yang telah dibentuk dengan beberapa komputer atau antar komputer yang menggunakan peralatan non-komputer, seperti: telpon selular, PDA, printer, handphone, mesin fax. Cakupan dari area sendiri sangatlah terbatas dengan jarak 9-10 meter. PAN juga dapat di bentuk dengan menggunakan teknologi *wire* dan *wireless network*. Dari teknologi *wire* PAN dapat disambungkan dengan menggunakan USB dan

FireWire dan sedangkan *wireless* PAN dapat disambungkan dengan menggunakan *Infrared, Bluetooth* dan WiFi.

Adanya dua jaringan *peer-to-peer* (P2P) merupakan kedudukan komputer yang terhubung sama pada setiap jaringan komputer dan sedangkan *client-server* adanya sebuah komputer yang dapat mengatur semua fasilitas seperti komunikasi, penggunaan pada perangkat kerang dan lunak dapat bersamaan dan dapat mengontrol jalannya jaringan.

Agar jaringan komputer dapat aman perlu adanya keamanan pada jaringan komputer seperti *Firewall. Firewall* tersebut merupakan suatu sistem atau perangkat yang memberikan izin lalu lintas pada jaringan yang dianggap aman untuk dilalui dan dapat mengantisipasi atau mencegah adanya lalu lintas jaringan yang sifatnya tidak aman yang dipisahkan antara jaringan lokal dengan jaringan publik dengan memakai metode filtering paket data yang masuk dan keluar.



Gambar 2.3 Jenis Firewall

Sumber: I Gede Suputra Widharma (2020)

Firewall dapat melakukan mengatur dan mengontrol lalu lintas yang sedang terjadi pada jaringan yang dibeikan izin untuk dapat mengakses jaringan pivat oleh *firewall.* Dari *firewall* dapat melakukan inspeksi pada paket dan memantau pada koneksi yang kemudian melakukan *filtering*

pada koneksi yang berdasarkan hasil inspeksi paket. Yang kedua adanya autentikasi pada akses, yang ketiga mencatat semua kejadian yang keempat dapat melaporkan kepada administraor, yang kelima agar pengguna tidak diarahkan pada situs yang berbahaya, yang keenam dapat memblokir situs tertentu, yang ketujuh menghindari adanya pembajakan pada pengguna komputer dengan menggunakan jaringan komputer dan yang terakhir adalah dapat menjaga sumber daya pada jaringan privat.

Firewall yang diterapkan pada mesin terdedikasi dapat berjalan ke pintu gerbang (*gateway*) antara jaringan lokal satu dengan jaringan lainnya dan dapat mengontrol akses kepada siapa saja yang dapat mengakases jaringan pribadi dari pihak luar. Menurut I Gede Suputra Widharma (2020) Terdapat 2 jenis *firewall*, yaitu :

a. *Personal Firewall*

   Personal firewall yang didesain untuk dapat menjaga dan melindungi sebuah komputer yang telah terhubung ke jaringan dari akses yang tidak dikehendaki. *Personal firewall* mempunyai dua fitur utama yaitu *Packet Filter Firewall* dan *Stateful Firewall.* Jenis dari *firewall* ini telah berkembang menjadi kumpulan program yang memiliki tujuan untuk menjaga dan mengamankan komputer dengan total yang kemudian ditambahkan dengan beberapa fitur pengaman perangkat untuk proteksi terhadap *anti-spyware*, *anti-spam*, virus dan ada beberapa produk dari *firewall* telah dilengkapi dengan manfaat dari pendeteksian gangguan keamanan jaringan (*Intrusion Detection System*).

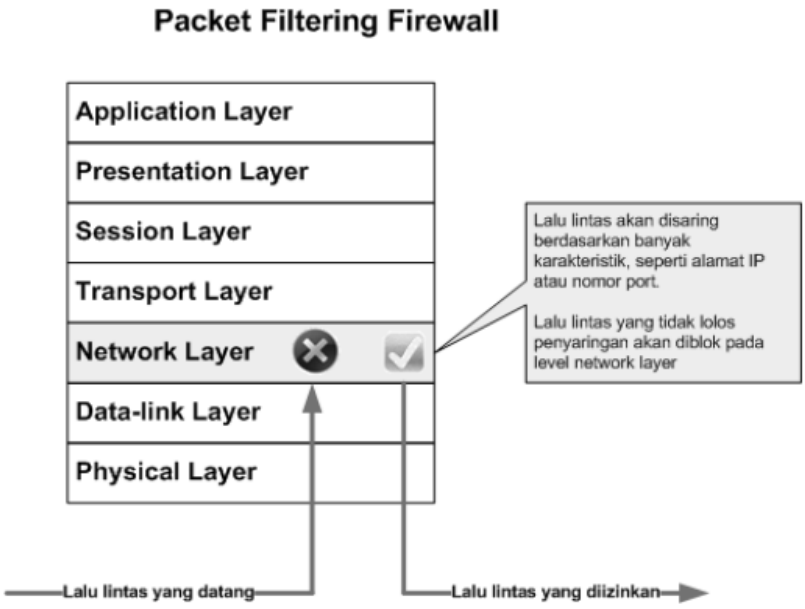
b. *Network Firewall*

   Network Firewall didesain guna menjaga dan melindungi jaringan yang menyeluruh dari semua serangan. *Network Firewall* memiliki sifat yang transparan dari pengguna dan memakai teknologi *routing* untuk dapat menentukan paket mana yang diberikan izin dan yang mana yang ditolak. Dari *Network Firewall* memiliki 2 bentuk yaitu

sebuah perangkat lunak yang telah diinstalasikan seperti: *Microsoft Internet Security* and *Acceleration Server* (ISA *Server*), Cisco ASA, IPTables pada sistem operasi GNU/Linux, Cisco PIX dan pf pada keluarga sistem operasi Unix BSD. Sedangkan SunScreen dari Sun Microsystems, Inc di bundel pada sistem operasi Solaris. Fitur utama yang dimiliki seperti: *Circuit Level Gateway, packekt filter firewall* dan *stateful firewall, NAT Firewall* dan *Application Level Gateway*.

Menurut I Gede Suputra Widharma (2020) Terdapat beberapa cara kerja dari *Firewall,* seperti:

1) Packet-Filter Firewall



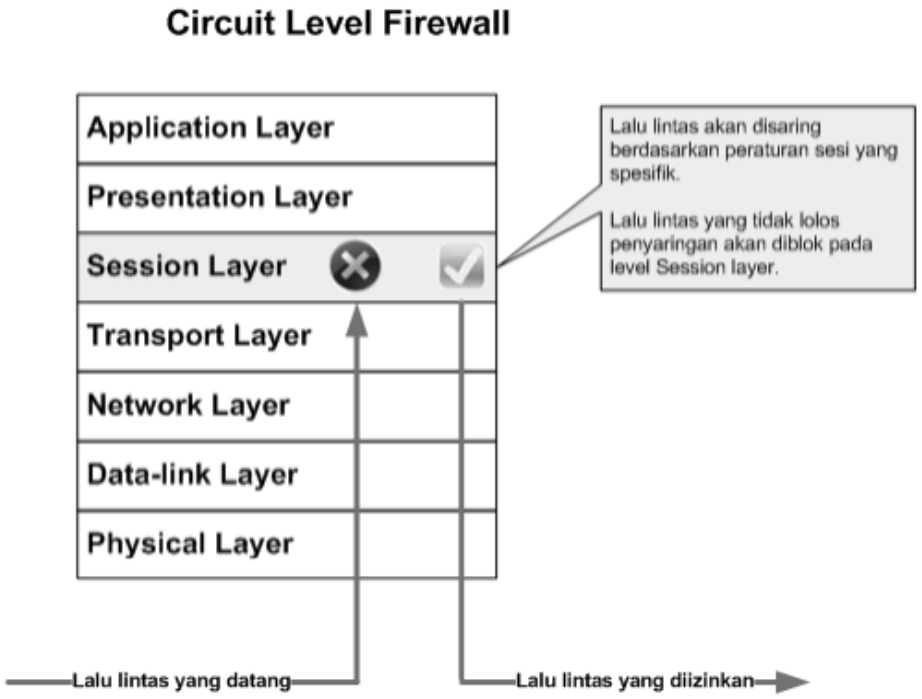
Gambar 2.4 *Packet Filter Firewall*

Sumber: Dalam jurnal Bina Nusantara (2010)

Sebuah *firewall* sama dengan sebuah *router* yang dilengkapi oleh dua buah *Network Interface Card* (NIC) kartu antar muka yang dapat melakukan *filtering* paket yang masuk. Cara kerjanya dengan membandingkan alamat sumber dari paket yang dibantu dengan kebijakan pengontrolan akses yang sudah terdaftar pada *Access Control List Firewall, router* ini yang nanti nya mencoba menghentikan atau memutuskan apakah paket tersebut dapat

masuk atau tidak pada tujuannya. Mungkin dapat menguji dari alamat IP yang menjadi sumber paket dan menentukan paket tersebut dapat dieruskan atau tidak. Hal ini dapat mengaktifkan/menonaktifkan port TCP/IP pada sistem *firewall.* Manfaat dari penggunaan ini dapat memberikan keamanan yang lebih kuat namun memiliki kelemahan seperti: kerumitan pada konfigurasi dari daftar *Access Control List Firewall* yang membesar dikarenakan banyak alamat IP, *exception* yang diberlakukan, *port* dimasukan kedalam dan nama domain.

2) *Circuit Level Gateway*

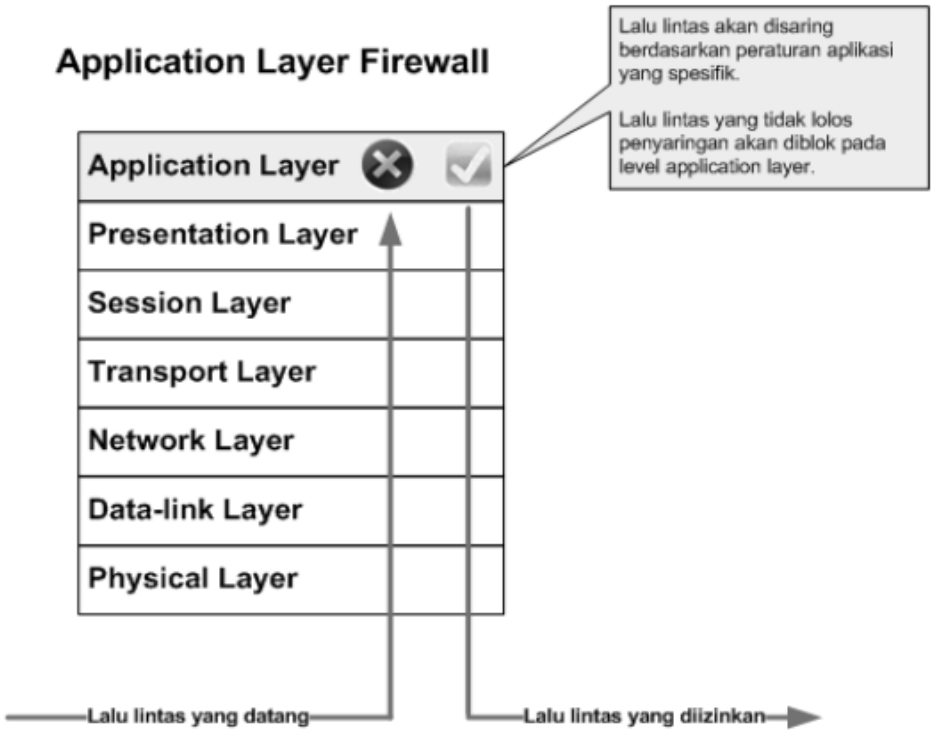


Gambar 2.5 *Circuit Level Firewall*

Sumber: Dalam jurnal Bina Nusantara (2010)

Circuit Level Gateway merupakan komponen di dalam *proxy server*. Jenis operasi ini sangat tinggi pada model referensi tujuh lapis OSI dan lebih aman dikarenakan pengguna eksternal nya tidak dapat terlihat dari IP jaringan internal pada paket yang di terima dari pada *Packet Filtering Firewall* dan memiliki rangka penyembunyian informasi jaringan proteksi yang meskipun tidak melakukan *filtering* pada paket individual yang ada pada koneksi. Koneksi ini antara pengguna dan jaringan yang nantinya disembunyikan dari pengguna. Pengguna akan menggunakan *firewall* ketika saat proses pembuatan koneksi, *firewall* akan menghasilkan koneksi dari sumber daya jaringan yang akan diakses oleh si pengguna setelah merubah alamat IP pada paket yang sudah di transmisi dari kedua belah pihak. Ini mengakibatkan terjadinya sirkuit virtual antara pengguna dengan sumber daya jaringan yang di akses.

3) Applicaition Level Firewall



Gambar 2.6 *Appliciation Layer Firewall*

Sumber: Dalam jurnal Bina Nusantara (2010)

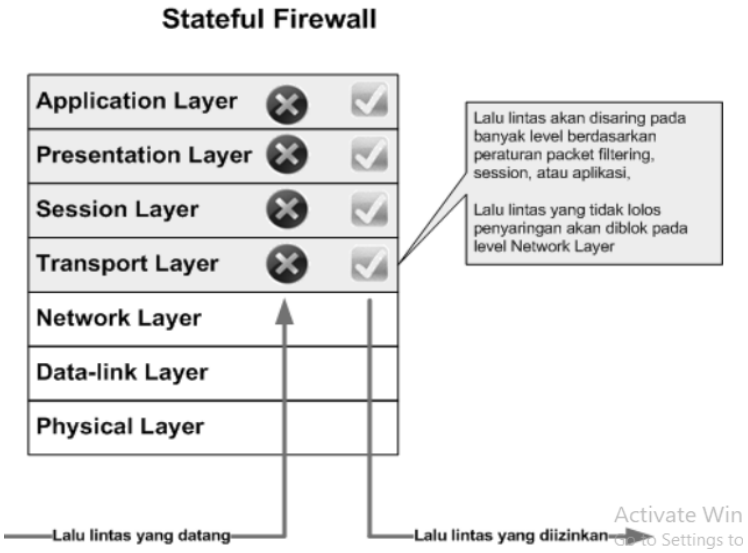
Applicaition Level *Firewall* sama dengan *proxy firewall* yang mana tidak mengizinkan paket yang akan datang untuk dapat melewati *firewall* langsung. Sebelumnya *firewall* ini melakukan autentikasi dahulu sebelum diizinkan mengakses jaringan dan mengharuskan beberapa konfigurasi harus diberlakukan pada pengguna agar dapat berfungsi. Aplikasi *proxy* dapat berjalan dalam komputer yang bekerja pada *firewall* yang nantinya akan dapat meneruskan permintaan pada layanan yang tersedia pada jaringan privat dan kemudian meneruskan kembali respon dari permintaan pada komputer yang menghasilkan permintaan pertama kali yang terletak pada jaringan publik yang tidak aman. Jenis ini melakukan implementasi *auditing* dan pencatatan (*logging*) yang menjadikan suatu kebijakan kemanan yandi terapkan.

4) *NAT* (*Network Adress* Translation) *Firewall*

NAT Firewall yang otomatis memberikan layanan proteksi pada sistem yang berada di balik *firewall* karena hanya NAT yang mengizinkan koneksi yang dalam dari komputer yang berada dibalik *firewall* dan memiliki tujuan dapat melakukan *multiplexing* pada lalu lintas dari jaringan internal yang kemudian memberikan ke jaringan yang lebih luas seperti MAN, WAN atau internet yang seakan-akan paket datang dari alamat IP atau alamat lainnya. Dari NAT sendiri juga membuat tabel memori yang berisi informasi mengenai koneksi yang dilihat dari *firewall* dan langsung dipetakan pada alamat jaringan internal ke eksternal. Kemampuannya dalam menaruh semua jaring di belakang alamat IP disebabkan adanya pemetaan dari *port* sampai NAT dalam Bina Nusantara (2010).

5) *State Firewall*

State Firewall suatau bentuk dari *firewall* yang dapat menyatukan keunggulan yang di tawari oleh *packet-filtering firewall, NAT Firewall, Circuit-Level Firewall* dan *Proxy Firewall* di satu sistem dan didesain lebih transparan. Dari sini dapat melakukan penyaringan pada lalu lintas yang didasarkan pada karakter si paket seperti *packet-filtering firewall* dan mempunyai pengecekan pada sesi koneksi yang memberikan keyakinan bahwa sesi koneksi telah terbentuk dan diizinkan. Ini juga termasuk pada beberapa aspek yang dimiliki *application level firewall* karena disini telah melakukan inspeksi pada data yang datang dari lapisan aplikasi dan hanya tersedia di beberapa *firewall* level atas saja, seperti Cisco PIX yang dikarenakan dapat menyatukan keunggulan dari jenis *firewall* lain dan *state firewall* menjadi lebih kompleks dalam Bina Nusantara (2010).



Gambar 2.7 *State Firewall*

Sumber: Dalam jurnal Bina Nusantara (2010)

2.2 Penelitian Terdahulu Yang Relevan

Sebelum peneliti memaparkan analisis dalam penelitian. Terdapat adanya beberapa literatur penelitian yang menggunakan bahasan tentang strategi pertahanan dalam membangun sistem guna menghadapi ancaman siber, sebagai bahan perbandingan dan referensi. Penelitian yang dilakukan harus berdasarkan pada hasil penelitian sebelumnya yang relevan. Beberapa penelitian tersebut antara lain:

a. Adi Rio Arianto dan Gesti Anggaraini (2019)

Penellitian yang dilakukan oleh Adi Rio Arianto dan Gesti Anggaraini (2019) dengan judul "Membangun Pertahanan dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia *Security Incident Response Team On Internet Infrastructure (ID-SIRTII)*", menunjukkan bahwa terbentuknya adanya Indonesia *Security Incident Response Team On Internet Infrastructure (ID-SIRTII)* yang menjadikan strategi pada instantsi Kementerian Komunikasi dan Informatika Republik Indonesia dalam bentuk stabilitas informasi dan perlindungan dari serangan dan ancaman siber.

b. Nur Khalimatus Sa'diyah dan Ria Tri Vinata (2016)

Penellitian yang dilakukan oleh Nur Khalimatus Sa'diyah dan Ria Tri Vinata (2016) dengan judul "Rekonstruksi Pembentukan *National Cyber Defense* Sebagai Upaya Mempertahankan Kedaulatan Negara". Menunjukkan bahwa dengan melakukan rekonstruksi dalam pembentukan *national cyber defense* atau *cyber war* guna melindungi data informasi rahasia negara , mempertahankan dan menjaga kedaulatan negara yan sesuai dengan UU No. 3 Tahun 2002 mengenai Pertahanan Negara yang didalamnya menyangkut adanya ancaman militer dan non militer yang salah satu nya adalah ancaman siber.

c. Rifani Agnes Eka Wahyuni, Surryanto Djoko Waluyo, dll (2021)

Penellitian yang dilakukan oleh Rifani Agnes Eka Wahyuni, Surryanto Djoko Waluyo, dll (2021) dengan judul "*Strengthening The Cyber Defence Center Of The Ministry Of Defence Of The Republic Of Indonesia* (PUSDATIN KEMHAN) *To Support The Indonesian Defense Diplomacy In Cyber Defese Security Cooperation In ASEAN"*. Menunjukkan bahwa pemerintah Indonesia melihat dan memahami kondisi untuk dapat mengamankan Indonesia dari adanya ancaman siber dan demi mewujudkan pembangunan pertahanan Indonesia.

d. Ratno Dwi Putra, Supartono, dll (2018)

Penellitian yang dilakukan oleh Ratno Dwi Putra, Supartono, dll (2018) dengan judul "Ancaman Siber Dalam Perspektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta)". Menunjukkan bahwa Internet menjadi penemuan terbesar yang telah memberikan banyak manfaat dan tantangan. Para pemangku khusus nya TNI yang melibatkan pertahanan siber terdapatnya pengembangannya pada pertahanan semesta yang dapat melakukan tugas pokoknya sebagai TNI.

e. Eko Budi, Dwi Wira, dll (2021)

Penellitian yang dilakukan oleh Eko Budi, Dwi Wira, dll (2021) dengan judul "Strategi Penguatan *Cyber Security* Guna Mewujudkan Keamanan Nasional di *Era Society 5.0*". Menunjukkan bahwa adanya konsep dari *Society 5.0* telah terpusat pada manusia dan teknologi yang tidak bisa dipisahkan yang dikarenakan industri sendiri adalah penggerak utama dari teknolgi dan manusia yang modern. Keamanan siber berperan penting dan vital dalam mencegah terjadinya kejahatan siber. Pada kondisi pandemi *Covid-19* yang telah dimanfaatkan oleh para peretas untuk melakukan aksi kejahatannya pada dunia siber.

Tabel 2.2 Penelitian Terdahulu

No	Nama	Judul Penelitian	Metode	Hasil Penelitian	Persamaan	Perbedaan
1	Adi Rio Arianto dan Gesti Anggaraini (2019)	Membangun Pertahanan dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia *Security Incident Response Team On Internet Infrastructure (ID-SIRTII)*	Kualitatif, dengan Konsep Geometripolitika dan fungsionalisme	Hasil penelitian menunjukkan bahwa adanya terbentuknya adanya Indonesia *Security Incident Response Team On Internet Infrastructure (ID-SIRTII)* yang menjadikan strategi pada instansi Kementerian Komunikasi dan	Melakukan penguatan pertahanan siber dan membangun sistem siber guna menghadapi ancaman siber	Peneliti membahas mengenai membangun pertahanan siber yang menggunakan Geometripolitika dan fungsionalisme guna menghadapi ancaman siber

				Informatika Republik Indonesia dalam bentuk stabilitas informasi dan perlindungan dari serangan dan ancaman siber. Dengan penggunaan geometripolitika dan fungsionalisme menjadikan formulasi dan aktivasi kekuatan pada bidang siber, melakukan		

				pencegahan dan ancaman yang nantinya dapat menciptakan struktur pertahanan dan keamanan siber nasiona Indonesia.		
2	Nur Khalimatus Sa'diyah dan Ria Tri Vinata (2016)	Rekonstruksi Pembentukan *National Cyber Defense* Sebagai Upaya Mempertahankan Kedaulatan Negara	Kualitatif, Konsep Keamanan *Cyber*, Konsep Pertahanan Negara	Hasil penelitian menunjukkan bahwa melakukan rekonstruksi dalam pembentukan *national cyber defense* atau	Dengan adanya ancaman serangan siber atau *cyber war* maka pemerintah melakukan peningkatan kemampuan di	Peneliti membahas mengenai Dengan adanya ancaman serangan siber atau *cyber war* maka dibentuknya

				cyber war guna melindungi data informasi rahasia negara , mempertahankan dan menjaga kedaulatan negara yan sesuai dengan UU No. 3 Tahun 2002 mengenai Pertahanan Negara yang didalamnya menyangkut adanya ancaman militer dan non militer yang salah satu	bidang siber untuk melindungi kedaulatan wilayah, keutuhan wilayah dan keselamatan bangsa Indonesia.	*National Cyber Defense (Cyber Army)* dan bekerja sama dengan lembaga-lembaga yang berkecimpung di dunia siber.

				nya adalah ancaman siber.		
3	Rifani Agnes Eka Wahyuni, Surryanto Djoko Waluyo, dll (2021)	*Strengthening The Cyber Defence Center Of The Ministry Of Defence Of The Republic Of Indonesia* (PUSDATIN KEMHAN) *To Support The Indonesian Defense Diplomacy In Cyber*	Kualitatif, Konsep Proteksi dan Konsep *Cyber Defense*	Hasil penelitian menunjukkan bahwa adanya pemerintah Indonesia melihat dan memahami kondisi untuk dapat mengamankan Indonesia dari	Memperkuat sistem keamanan siber guna melindungi kedaulatan wilayah, dan segenap bangsa Indonesia dalam menghadapi	Peneliti membahas mengenai penguatan di bidang siber dengan melakukan diplomasi pertahanan Indonesia yang dilakukan oleh

		Defese Security Cooperation In ASEAN		adanya ancaman siber dan demi mewujudkan pembangunan pertahanan Indonesia.	ancaman asimetris	Pushansiber untuk kerjasama keamanan siber dengan ASEAN
4	Ratno Dwi Putra, Supartono, dll (2018)	Ancaman Siber Dalam Perspektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta)	Kualitatif, Teori *National Defense Strategy*	Hasil penelitian menunjukkan bahwa Internet menjadi penemuan terbesar yang telah memberikan banyak manfaat dan tantangan. Para pemangku khusus nya TNI	Memperkuat sistem keamanan siber khusus nya dilingkungan TNI guna membangun dan mengembangkan keamanan dan pertahanan negara dengan	Peneliti membahas mengenai sistem pertahanan negara yang sifatnya semesta guna menghadapi ancaman siber

				yang melibatkan pertahanan siber terdapatnya pengembangan nya pada pertahanan semesta yang dapat melakukan tugas pokoknya sebagai TNI.	menggunakan sistem siber.	
5	Eko Budi, Dwi Wira, dll (2021)	Strategi Penguatan *Cyber Security* Guna Mewujudkan Keamanan Nasional di *Era Society 5.0*	Kualitatif, Teori strategi keamanan, *cyber security concept*	Hasil penelitian menunjukkan bahwa adanya menunjukkan bahwa adanya konsep dari *Society 5.0* telah	Melakukan penguatan strategi *cyber security* di Indonesia dalam tujuan	Peneliti membahas mengenai penguatan keamanan pertahanan pada kondisi pandemi

			dalam keamanan nasional, teori manajemen teknologi informasi, teori teori *cyber attack*	terpusat pada manusia dan teknologi yang tidak bisa dipisahkan yang dikarenakan industri sendiri adalah penggerak utama dari teknologi dan manusia yang modern. Keamanan siber berperan penting dan vital dalam mencegah terjadinya	keamanan nasional	*covid-19* yang di manfaatkan oleh peretas.

				kejahatan siber. Pada kondisi pandemi *Covid-19* yang telah dimanfaatkan oleh para peretas untuk melakukan aksi kejahatannya pada dunia siber.		

Sumber: diolah peneliti 2022

Dari penelitian terdahulu yang telah di jelaskan pada tabel diatas, menurut peneliti jurnal dari penelitian terdahulu yang mendekati dengan penulisan ini adalah jurnal dari Eko Budi, Dwi Wira, dll (2021) yang melakukan penguatan dan membangun sistem siber guna menjaga dan melindungi segenap bangsa Indonesia terhadap adanya ancaman siber.

Dari beberapa penelitian yang digunakan sebagai tinjauan, penulis fokus dalam segi objek penelitian yang memiliki perbedaan dengan penelitian sebelumnya, yaitu tentang membangun sistem siber guna menghadapi ancaman siber. Selain itu peneliti juga fokus pada bagaimana strategi pertahanan negara siber dalam menghadapi ancaman siber di Pushansiber.

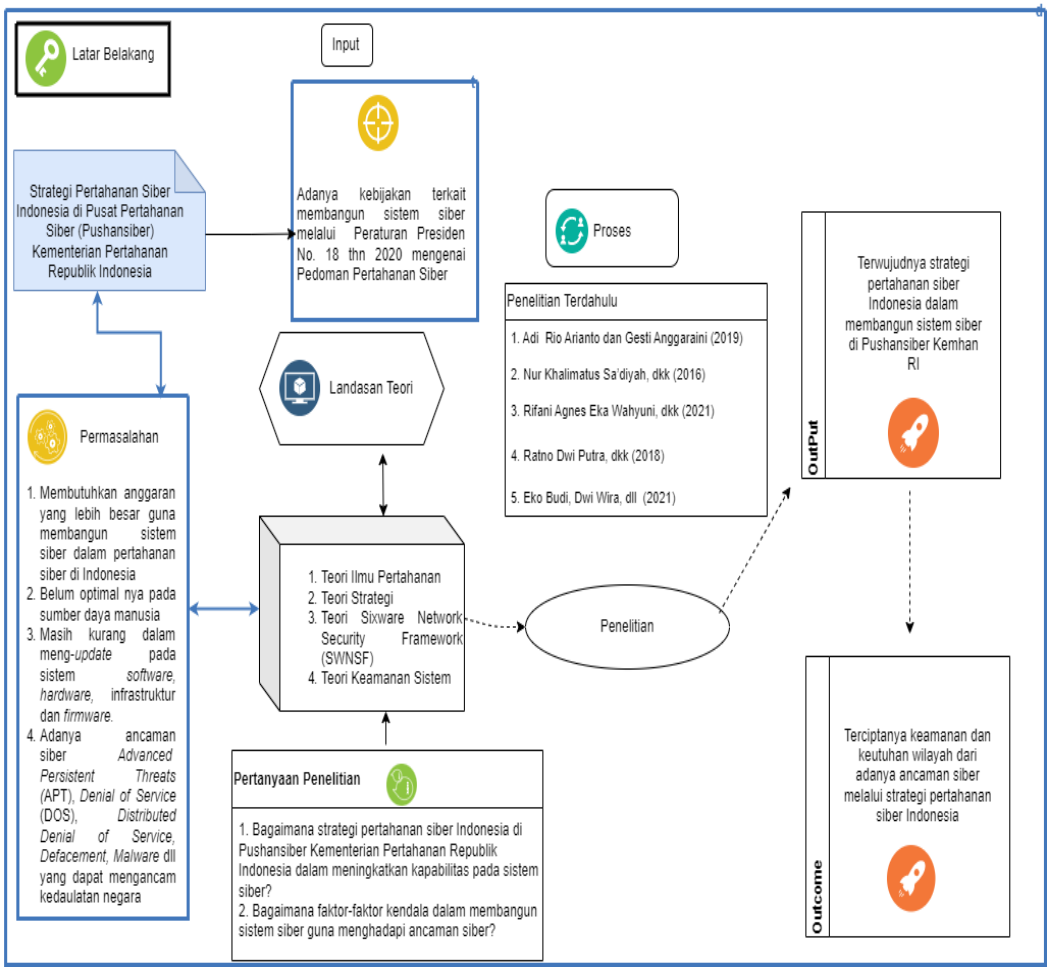
2.3 Kerangka Berpikir

Dalam kerangka berpikir ini, peneliti mendasarkan pemikiran pada tujuan nasional yang tercantum pada pembukaan Undang-Undang Dasar 1945, bahwa melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa serta ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial. Pada pembukaan Undang-Undang Dasar 1945 telah jelas disebutkan bahwa salah satu tujuan nasional Indonesia adalah untuk melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dengan cara memberikan perlindungan fisik bangsa dan wilayah Indonesia dari ancaman kekuatan yang berasal dari luar serta perlindungan hak setiap warga, komunitas, dan wilayah dari kemungkinan eksploitasi oleh pihak manapun. Terlebih situasi pada saat ini dengan dimensi ancaman yang semakin berkembang sesui dengan lingkungan global dan kecanggihan teknologi dan informasi.

Didalam buku Pedoman Pertahanan Siber (2014), dijelaskan bahwa ruang siber perlu menerima perlindungan yang kuat guna menghindari adanya potensi yang dapat memberikan kerugian dan menghancurkan kedaulatan siber nasional. Telah tertuang pada Undang-Undang Republik Indonesia No 3 Tahun 2002 tentang Pertahanan Negara yang memiliki tujuan untuk dapat menjaga dan melindungi kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia dan keselamatan segenap bangsa dari bentuk ancaman baik dari militer dan non-militer terutama di ruang siber dalam kemampuan *soft* dan *smart power* pertahanan yang harus di tingkatkan melalui strategi penindakan, penangkalan dan pemulihan pertahanan siber (*cyber defense*) guna menuju kedaualatan siber nasional dalam Pedoman Pertahanan Siber (2014).

Dilihat dari sisi kesiapan pemerintah Indonesia dalam menghadapi dampak ancaman siber, peneliti melihat bahwa pemerintah masih belum optimal dalam membangun sisitem siber. Terlebih saat ini ancaman siber memunculkan celah baru masuknya serangan dengan timbulnya beberapa ancaman dengan melalui beberapa cara yang dilakukan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, peneliti memutuskan untuk meneliti terkait bagaimana Strategi Pertahanan Siber Indonesia Suatu Studi di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia.

Berikut ini adalah Gambar bagan kerangka berpikir peneliti secara keseluruhan, yang melingkupi teori dan konsep yang pada bab selanjutnya akan dibahas lebih mendalam.



Gambar 2.8 Kerangka Berpikir

Sumber: diolah peneliti 2022