4.2.3 Dokumentasi

Peneliti telah melaksanakan pengecekan dokumentasi melihat dan mengamati pada pedoman pertahanan siber pada Permenhan No. 82 Tahun 2014 dalam membangun dan meningkatkan kapabilitas pada sistem siber. Pengecekkan pada dokmentasi yang berada di lokasi penelitian yaitu di Gedung Pusat Pertahanan Siber di Lantai 4 bersama Bapak Kolonel Sus Tri Satya sebagai Kepala Bidang Penjamin Operasi Siber dan beserta Bapak Irfan Mountini, S. Kom yang memiliki jabatan sebagai Pranata Komputer Madya Pusat Pertahanan Siber, Bapak Rudy Wahyudi, S. Kom., M. Han yang memiliki jabatan sebagai Kepala Subbidang Keamanan Infrastruktur dan Komputer Bidang Penjamin Keamanan Pusat Pertahanan Siber dan Bapak Eko Joko Murwanto, S. Kom., M.Si yang memiliki jabatan sebagai Kepala Sub bidang Keamanan Aplikasi Bidang Penjamin Keamanan Pusat Pertahanan Siber. Adapun hal-hal yang peneliti dokumentasi sesuai dengan tujuan dari penelitian: 1) Permenhan No. 82 Tahun 2014; 2) Peraturan Presiden Republik Indonesia No. 18 Tahun 2020 mengenai Rencana Pembangun Jangka Menengah Nasional Tahun 2020-2024.

4.3 Hasil Pengolahan Data

Pada tahap pengolahan data ini, peneliti telah melakukan pemeriksaan atas jawaban dari hasil beberapa informan dan telah mengelompokkan jawaban yang sesuai dengan pertanyaan penelitian. Tujuannya merupakan memberikan penghalusan pada data berikutnya telah memberikan keterangan tambahan dan mengeliminasi yang tidak penting. Proses menurut dari Miles dan Huberman disebut dengan kondensasi data (Miles, Huberman, & Saldana, 2014), dari kondensasi data ini yang mengarah pada hal yang penting, terdapat nya kata kunci dan mencari tema dari polanya. Kondensasi data dapat memberikan gambaran yang lebih jelas.

4.3.1 Faktor-Faktor Kendala Dalam Membangun Sistem Siber Guna Menghadapi Ancaman Siber

Hasil dari wawancara kepada beberapa narasumber yang menunjukkan bahwa di Pushansiber memiliki faktor kendala dalam membangun sistem siber. Gambaran ini mengenai terdapatnya faktor yang menjadi kendala bagi Pushansiber dalam melakukan membangun sistem siber dalam konsep pertahanan siber. Peneliti melakukan penelitian dengan menggunakan wawancara kepada beberapa narasumber dari Pushansiber, mantan kepala Kapusdatin dan pakar teknologi informatika dan studi Pustaka. Berdasarkan penelitian tersebut, telah mendapatkan hasil bahwa terdapatnya faktor kendala dalam membangun sistem siber di Pushansiber.

Peneliti melakukan wawancara dengan Bapak Irfan Mountini, S. Kom yang memiliki jabatan sebagai Pranata Komputer Madya Pusat Pertahanan Siber, kemudian dengan Bapak Rudy Wahyudi, S. Kom., M. Han yang memiliki jabatan sebagai Kepala Subbidang Keamanan Infrastruktur dan Komputer Bidang Penjamin Keamanan Pusat Pertahanan Siber dan juga dengan Bapak Eko Joko Murwanto, S. Kom., M.Si yang memiliki jabatan sebagai Kepala Subbidang Keamanan Aplikasi Bidang Penjamin Keamanan Pusat Pertahanan Siber.

Mereka mengatakan bahwa di Pushansiber memiliki faktor kendala yang sangat besar maka dari itu dapat memberikan dampak dalam melakukan tugas di Pushansiber. Terdapat penjelasan dari faktor kendala yang dimiliki oleh Pushansiber dibawah ini, seperti:

a. Pada sumber daya manusia di Pushansiber memiliki penurunan pada kemampuan dan keahlian di bidang siber. Pemberian pelatihan, sertifikasi internasional, pendidikan dan lain-lain masih sangat belum cukup maka dari itu penguasaan pada *technology security* masih sangat jauh. Ditambah dengan kondisi pada saat ini terdapatnya pandemi *covid-19* yang menghambat pembangunan dan peningkatan dalam kemampuan sdm nya. Ruang gerak di perkecil dan semua kegiatan menjadi tidak jalan dan tersendat.

b. *Hardware* yang dimiliki oleh Pushansiber masih menggunakan perangkat yang lama, dan bahkan ada yang sudah tidak dapat dipakai atau dioperasikan.
c. Software yang dimiliki oleh Pushansiber juga masih memakai yang lama dan memakai aplikasi yang sifatnya *open source*. Belum dapat melakukan pengembangan atau inovasi pada aplikasi nya
d. Infrastruktur di Pushansiber masih banyak yang perlu di lengkapi untuk dapat menunjang pengoperasian dalam pertahanan siber
e. Pushansiber memiliki *Frameware* nya masih terbatas dan lama.
f. Pada tahun 2016 hingga sekarang, Pushansiber belum memiliki anggaran khusus siber untuk dapat menunjang pertahanan sistem siber. Kami telah membuat perencanaan strategi dari 2020-2024, namun belum dapat direalisasikan dalam pembangunan dan pengembangan kembali untuk sistem siber.

Peneliti melakukan wawancara dengan Bapak Dr. Ir. Achmad Farid W, M. yang memiliki jabatan sebagai dosen di perguruan tinggi Universitas Pertahanan Republik Indonesia sekaligus mantan dari Kepala *Cyber Defense* Pusat Data dan Informasi Kementerian Pertahanan. Beliau mengatakan bahwa di Pushansiber memiliki faktor kendala yang mengakibatkan kinerja nya menjadi menurun. Terdapat penjelasan dari faktor kendala yang dimiliki oleh Pushansiber dibawah ini, seperti:

a. Sumber daya Manusianya belum optimal dan belum siap dalam tingkat kemampuan di bidang siber. Masih ada personel dari Pushansiber yang belum memiliki kemampuan di bidang IT. Kejadian seperti ini saya sering temukan dan ini dapat memakan waktu yang lama untuk dapat memiliki keahlian di bidang IT. Kurangnya pelatihan dan pendidikan yang diberikan.
b. *Hardware* di Pushansiber ada yang tidak dapat beroperasi, rusak, dan lama. Ini dapat mempengaruhi durasi pengerjaan tugas untuk dapat diselesaikan secara tepat waktu, efisien dan efektif.

c. Software nya juga masih menggunakan yang lama dan tidak melakukan *update* pada aplikasi sehingga untuk dapat menggunakan aplikasi yang baru belum dapat digunakan dengan baik.
d. Infrastruktur nya pada Pushansiber perlu didukung dan sangat kurang baik. banyak yang sudah tidak aktif dan yang aktif hanya beberapa saja
e. *Firmware* yang di pakai masih lama dan belum adanya pembangunan dan pengembangan kembali.
f. Anggaran yang menjadi kendala besar di Pushansiber. Karena Pushansiber telah membuat perencanaan untuk pengembangan sistem siber agar dapat beroperasi dan siap. Pushansiber belum memiliki anggaran khusus siber, maka semua rencana tersebut belum dapat terprogramkan dengan baik. 2 tahun lebih terakhir ini di instansi Pushansiber tidak memiliki anggaran, yang seharusnya dapat anggaran, maka anggaran tersebut lebih di arahkan dan difokuskan pada kesehatan dan penyembuhan masyarkat Indonesia yang dikarenakan terkena nya penyakit *Covid-19.*

Peneliti melakukan wawancara dengan Bapak Prof. Dr. Ir. Richardus Eko Indrajit M. Sc., MBA., Mphil. MA yang memiliki jabatan sebagai pakar teknologi informatika. Beliau mengatakan bahwa terdapatnya faktor kendala yang dimiliki oleh Pushansiber. Pemerintah perlu memberikan dukungan, bantuan dan perhatian yang serius apabila ingin melakukan pembangunan dan pengembangan kembali. Terdapat penjelasan dari faktor kendala yang dimiliki oleh Pushansiber dibawah ini, seperti:

a. Kendalanya pada sumber daya manusia seperti kesiapannya, kemampuan dalam mengembangkan dan melaksanakan protokol pada keamanan siber yang menjadi kelemahan terbesar apabila tidak dukung dalam pengelolaan dengan bijaksana yang nanti nya dapat memberikan kerugian yang dikarenakan dapat diambil alih oleh pihak lain. Mulai dari tahun 2020 ketika *Covid-19* semua kegiatan menjadi terhambat dan pada sdm nya juga mengalami penurunan. Ini menjadi sangat berbahaya karena di manfaatkan oleh para penjahat siber ketika kemampuan yang dimiliki semakin menurun.
b. *Hardware* di Pushansiber ada yang tidak dapat beroperasi, dan lama.
c. Software nya juga masih menggunakan yang lama dan tidak melakukan *update*. *Open source* masih dilakukan.
d. Infrastruktur nya pada Pushansiber perlu dilengkapi dan ini menjadi bagian yang sangat vital dan kritis yang dikarenakan menyangkut pada aset, sistem, jaringan dan bentuk dari fisik yang lain
e. *Firmware* yang di pakai masih lama dan belum adanya pembangunan dan pengembangan kembali.
f. Anggaran yang menjadi kendala besar bagi Pushansiber. Apabila menginginkan sistem siber yang ideal, maka Pushansiber harus memiliki anggaran khusus untuk dapat mendukung kegiatan pertahanan siber.

Peneliti juga melakukan kajian mengenai dokumen-dokumen terkait yang diantaranya Pushansiber melakukan diskusi, kerja sama dengan negara lain, mengikuti seminar untuk meningkatkan kualitas, kemampuan dan keahlian pada sektor teknologi dan sumber daya manusia nya.

Gambar 4. 2 Wakil Menteri Pertahanan (Wamenhan) RI Melakukan Kunjungan Kerja Ke Pusat Pertahanan Siberr (Pushansiber).

Sumber: Kementerian Pertahanan Republik Indonesia (2019)

Pada gambar 4.2 Wamenhan melakukan kunjungan pada satuan kerja Pushansiber. Pada pertemuan tersebut, Wamenhan melihat pada fasilitas yang dimiliki oleh Pushansiber. Wamenhan menginginkan adanya pembangunan dan pengembangan kembali pada *hardware, software,* infrastruktur, dan *firmware* dan lebih memberikan penekanan pada sumber daya manusia nya agar kemampuan dan ilmu nya semakin meningkat dan kuat dalam mewujudkan pertahana siber yang baik dari segi teknologi dan sdm.

Gambar 4. 3 Pushansiber Menerima Kunjungan BSSN Terkait Identifikasi Sektor IIKN

Sumber: Kementerian Pertahanan Republik Indonesia (2019)

Pada gambar 4.3 telah melakukan penerimaan kunjungan dari pihak Badan Siber dan Sandi Negara (BSSN) guna mengkoordinasikan dalam pengidentifikasian sektor Infrastruktur Informasi Kritikal Nasional (IIKN). Dalam pertemuan ini membuat kesepakatan dalam kerjasama untuk daat berkolaborasi dan berkoordinasi dalam melakukan pengawasan pertahanan siber.

Gambar 4. 4 FGD Kajian Strategi Organisasi BSSN Dalam Rangka Mengonsolildasi Unsur Keamanan Siber

Sumber: Kementerian Pertahanan Republik Indonesia (2019)

Gambar 4.4 telah terdapat suatu kegiatan dalam menghadiri undangan dari pihak BSSN untuk agenda FGD kajian strategi. Ini menjadikan pengalaman dan mendapat ilmu yang dapat di terapkan pada Pushansiber guna melakukan pembangunan dan pengembangan kembali.

Peneliti juga mendapatkan data mengenai rencana strategi yang telah di buat oleh Kementerian Pertahanan Kementerian Pertahanan Republik Indonesia yang mana telah di konfirmasi oleh Bapak Rudy Wahyudi selaku Kepala Subbidang Keamanan Infrastruktur dan Komputer Bidang Penjamin Keamanan mengenai belum adanya anggaran khusus mengenai siber. Berikut gambar rencana strategi yang telah dibuat oleh Kementerian Pertahanan Republik Indonesia di bawah ini:

c. Kerangka Pendanaan Program TA 2022-2024.

No	Program	Indikasi Kebutuhan Pendanaan		
		2022	2023	2024
1	Dukungan Manajemen.	3.737.084.912.000	3.653.055.852.000	4.071.984.876.000
2	Kebijakan dan Regulasi Pertahanan.	32.118.186.000	32.118.186.000	32.118.186.000

No	Program	Indikasi Kebutuhan Pendanaan		
		2022	2023	2024
3	Modernisasi Alutsista, Non Alutsista, dan Sarpras Pertahanan.	29.123.450.042.000	18.228.153.075.577	18.249.734.912.951
4	Pembinaan Sumberdaya Pertahanan.	114.841.983.000	97.914.297.304	100.379.752.185
5	Riset, Industri, dan Pendidikan Tinggi Pertahanan.	4.633.746.792.000	913.064.551.000	909.151.692.000
Jumlah		37.165.555.507.000	22.924.305.961.881	23.363.369.419.136

Gambar 4. 5 Rencana Strategi Kementerian Pertahanan Republik Indonesia

Sumber: Kementerian Pertahanan Republik Indonesia

Dilihat dari gambar 4.5 Pushansiber belum terbentuk dari tahun 2013-2016, namun secara resmi Pushansiber terbentuk pada tahun 2017 dengan melalui permenhan 02/2017. Pada tahun 2017 juga belum mendapatkan anggaran. Selanjutnya terjadinya reorganisasi yang berada di Kemhan melalui Permenhan 14/2019. Pushansiber dari tahun 2019 hingga sekarang yang hanya mendapatkan anggaran untuk dapat melakukan pemeliharaan rutin seperti pemeliharaan gedung, perpanjangan lisesnsi dan kegaiatan rutin lainnya juga belum mendapatkan anggaran untuk melakukan pengembangan perangkat baik keras, lunak dan SDM nya. Terkait mengenai anggaran yang seharusnya dimiliki oleh Pushansiber harus melakukan aduit atau melakukan *assessment* kembali dengan kondisi saat ini yang mana sangat mahal untuk dapat melakukan pembangunan dan pengembangan kembali pada sistem siber yang ada di Pushansiber.

Peneliti juga mendapatkan dokumen Daftar Susunan Personel (DSP) mengenai sumber daya manusia yang dimiliki oleh pihak Pushansiber yang mana dari dsp Pushansiber tersebut menyatakan bahwa terdapatnya 179 orang tetapi baru terisi hanya 80 orang saja yang kemudian kemampuan yang dimiliki juga belum terpenuhi. Dilihat dari sisi jumlah tersebut dan kemampuannya memang sangat jauh dan belum siap dari sektor sumber daya manusianya. Berikut dibawah ini terlampir dokumen Daftar Susuna Personel (DSP) Pushansiber:

1. DAFTAR SUSUNAN PERSONEL

1	2	3	4	5	6	7	8	9	10	11	12	13
3.	**PUSAT PERTAHANAN SIBER**											
	Kepala Pusat Pertahanan Siber	-	1	-	-	-	-	-	1	IV/c - IV/d	Kolonel - Pati Bintang 1	
1	Analis Kebijakan Madya Bid Lola Sistem Han Siber			1	-	-	-	-	1	IV/a - IV/c	Letkol - Kolonel	
2	Analis Kebijakan Madya Bid Sistem Operasi			1	-	-	-	-	1	IV/a - IV/c	Letkol - Kolonel	
3	Analis Kebijakan Madya Bid Sistem Audit Tik			1	-	-	-	-	1	IV/a - IV/c	Letkol - Kolonel	
4	Analis Kebijakan Madya Bid Informasi Strategis Pertahanan di Daerah			3	-	-	-	-	3	IV/a - IV/c	Letkol - Kolonel	
5	Analis Kebijakan Muda Bid Lola Sistem Han Siber			-	1	-	-	-	1	III/c - III/d	Mayor - Letkol	
6	Analis Kebijakan Muda Bid Sistem Operasi			-	1	-	-	-	1	III/c - III/d	Mayor - Letkol	
7	Analis Kebijakan Muda Bid Sistem Audit Tik			-	1	-	-	-	1	III/c - III/d	Mayor - Letkol	
8	Pranata Komputer Tingkat Ahli								50			
	Pranata Komputer Madya				-	-	-	-	-	IV/a - IV/c	Letkol - Kolonel	
	Pranata Komputer Muda			-	-	-	-	-	-	III/c - III/d	Mayor - Letkol	
	Pranata Komputer Pertama			-	-	-	-	-	-	III/a - III/b	Letda - Kapten	
9	Pranata Komputer Tingkat Terampil								15			
	Pranata Komputer Penyelia			-	-	-	-	-	-	III/c - III/d	Kapten - Mayor	
	Pranata Komputer Pelaksana Lanjutan			-	-	-			-	III/a - III/b	Letda - Lettu	
	Pranata Komputer Pelaksana			-	-		-	-	-	II/b - II/d	Serka - Peltu	
	JUMLAH								**75**			

1	2	3	4	5	6	7	8	9	10	11	12	13
A	**BID TATA KELOLA DAN KERJA SAMA**											
	Kabid Tata Kelola dan Kerja Sama	-	-	1	-	-	-	-	1	IV/a - IV/c	Letkol - Kolonel	
A1	**SUBBID TATA LAKSANA DAN KERJA SAMA**											
	Kasubbid Tata Laksana dan Kerja Sama	-	-	-	1	-	-	-	1	III/c - III/d	Mayor - Letkol	
1	Penyusun Naskah			-	-	1	-	-	1	III/c - III/d	Kapten - Mayor	
2	Pengolah Data			-	-	1	-	-	1	III/b - III/c	Lettu - Kapten	
3	Pengelola Data			-	-	1	-	-	1	III/b - III/c	Letda - Lettu	
4	Pengadministrasi Umum			-	-	-	1	-	1	II/a - II/d	Serda - Peltu	
5	Pranata Teknologi Informasi Komputer			-	-	-	1	-	1	II/a - II/d	Serda - Peltu	
	JUMLAH A1								6			
A2	**SUBBID PERENCANAAN**											
	Kasubbid Perencanaan	-	-	-	1	-	-	-	1	III/c - III/d	Mayor - Letkol	
1	Analis Perencanaan			-	-	1	-	-	1	III/c - III/d	Kapten - Mayor	
2	Pengolah Data			-	-	1	-	-	1	III/b - III/c	Lettu - Kapten	
3	Pengelola Data			-	-	1	-	-	1	III/a - III/b	Letda - Lettu	
4	Pranata Teknologi Informasi Komputer			-	-	-	1	-	1	II/a - II/d	Serda - Peltu	
	JUMLAH A2								5			
A3	**SUBBID IMPLEMENTASI DAN PEMELIHARAAN**											
	Kasubbid Implementasi dan Pemeliharaan	-	-	-	1	-	-	-	1	III/c - III/d	Mayor - Letkol	
1	Penyusun Naskah			-	-	2	-	-	2	III/c - III/d	Kapten - Mayor	

Gambar 4. 6 Daftar Susunan Personel di Pushansiber Kemhan RI

Sumber: Pushansiber KEMHAN RI

1	2	3	4	5	6	7	8	9	10	11	12	13
B3	**SUBBID DIGITAL FORENSIK DAN PEMULIHAN**											
	Kasubbid Digital Forensik dan Pemulihan	-	-	-	1	-	-	-	1	III/c - III/d	Mayor - Letkol	
1	Penyusun Naskah			-	-	1	-	-	1	III/c - III/d	Kapten - Mayor	
2	Pengolah Data			-	-	6	-	-	6	III/b - III/c	Lettu - Kapten	
3	Pengelola Laboratorium			-	-	5	-	-	5	III/a - III/b	Letda - Lettu	
4	Pengelola Data			-	-	1	-	-	1	III/a - III/b	Letda - Lettu	
5	Pranata Teknologi Informasi Komputer			-	-	-	1	-	1	II/a - II/d	Serda - Peltu	
	JUMLAH B3								15			
	JUMLAH BID OPERASI SIBER								38			
C	**BID PENJAMINAN KEAMANAN**											
	Kabid Penjaminan Keamanan	-	-	1	-	-	-	-	1	IV/a - IV/c	Letkol - Kolonel	
C1	**SUBBID KEAMANAN INFRASTRUKTUR DAN KOMUNIKASI**											
	Kasubbid Keamanan Infrastruktur dan Komunikasi	-	-	-	1	-	-	-	1	III/c - III/d	Mayor - Letkol	
1	Penyusun Naskah			-	-	2	-	-	2	III/c - III/d	Kapten - Mayor	
2	Pengolah Data			-	-	1	-	-	1	III/b - III/c	Lettu - Kapten	
3	Pengelola Data			-	-	2	-	-	2	III/a - III/b	Letda - Lettu	
4	Pengadministrasi Umum			-	-	-	1	-	1	II/a - II/d	Serda - Peltu	
5	Pranata Teknologi Informasi Komputer			-	-	-	1	-	1	II/a - II/d	Serda - Peltu	
	JUMLAH C1								8			
	Pengolah Data			-	-	3	-	-	3	III/b - III/c	Lettu - Kapten	
	Pengelola Data			-	-	1	-	-	1	III/a - III/b	Letda - Lettu	
	Pranata Teknologi Informasi Komputer			-	-	-	1	-	1	II/a - II/d	Serda - Peltu	
	JUMLAH B2								7			

Gambar 4. 7 Daftar Susunan Personel di Pushansiber Kemhan RI

Sumber: Pushansiber KEMHAN RI

1	2	3	4	5	6	7	8	9	10	11	12	13
C2	SUBBID KEAMANAN APLIKASI											
	Kasubbid Keamanan Aplikasi	-	-	-	1	-	-	-	1	III/c - III/d	Mayor - Letkol	
1	Penyusun Naskah			-	-	1	-	-	1	III/c - III/d	Kapten - Mayor	
2	Pengolah Data			-	-	2	-	-	2	III/b - III/c	Lettu - Kapten	
3	Pengelola Data			-	-	1	-	-	1	III/a - III/b	Letda - Lettu	
4	Pranata Teknologi Informasi Komputer			-	-	-	1	-	1	II/a - II/d	Serda - Peltu	
	JUMLAH C2								6			
C3	SUBBID PENGEMBANGAN SIBER											
	Kasubbid Pengembangan Siber	-	-	-	1	-	-	-	1	III/c - III/d	Mayor - Letkol	
1	Penyusun Naskah			-	-	1	-	-	1	III/c - III/d	Kapten - Mayor	
2	Pengolah Data			-	-	3	-	-	3	III/b - III/c	Lettu - Kapten	
3	Pengelola Data			-	-	2	-	-	2	III/a - III/b	Letda - Lettu	
4	Pranata Teknologi Informasi Komputer			-	-	-	1	-	1	II/a - II/d	Serda - Peltu	
	JUMLAH C3								8			
	JUMLAH BID PENJAMINAN KEAMANAN								23			
D	SUBBAG TATA USAHA											
	Kasubbag Tata Usaha	-	-	-	1	-	-	-	1	III/c - III/d	Mayor - Letkol	
1	Penyusun Naskah			-	-	2	-	-	2	III/c - III/d	Kapten - Mayor	
2	Bendahara			-	-	1	-	-	1	III/c - III/d	Kapten - Mayor	
3	Pengolah Data			-	-	5	-	-	5	III/b - III/c	Lettu - Kapten	
4	Pengelola Data	-	-	-	-	5	-	-	5	III/a - III/b	Letda - Lettu	
5	Pengelola Kepegawaian			-	-	1	-	-	1	III/a - III/b	Letda - Lettu	
6	Sekretaris			-	-	-	1	-	1	II/a - II/d	Serda - Peltu	
7	Pengadministrasi Umum			-	-	-	2	-	2	II/a - II/d	Serda - Peltu	

1	2	3	4	5	6	7	8	9	10	11	12	13
8	Pengadministrasi Persuratan			-	-	-	1	-	1	II/a - II/d	Serda - Peltu	
9	Pengemudi VIP			-	-	-	1	-	1	II/a - II/d	Serda - Peltu	
10	Pranata Teknologi Informasi Komputer			-	-	-	1	-	1	II/a - II/d	Serda - Peltu	
	JUMLAH SUBBAG TU								21			
	JUMLAH PUS HANSIBER								179			

Gambar 4. 8 Daftar Susunan Personel di Pushansiber Kemhan RI

Sumber: Pushansiber KEMHAN RI

2. REKAPITULASI JABATAN PUS PERTAHANAN SIBER

NO	BAGIAN	JUMLAH			JUMLAH TOTAL	KET
		ESELON	FUNGSIONAL	PELAKSANA		
1	2	3	4	5	6	7
1	PUS PERTAHANAN SIBER					
	ESELON	1	-	-		
	FUNGSIONAL	-	74	-		
	PELAKSANA	-	-	-		
					75	
2	BID TATA KELOLA DAN KERJA SAMA					
	ESELON	4	-	-		
	FUNGSIONAL	-	-	-		
	PELAKSANA	-	-	18		
					22	
3	BID OPERASI SIBER					
	ESELON	4	-	-		
	FUNGSIONAL	-	-	-		
	PELAKSANA	-	-	34		
					38	
4	BID PENJAMINAN KEAMANAN					
	ESELON	4	-	-		
	FUNGSIONAL	-	-	-		
	PELAKSANA	-	-	19		
					23	

1	2	3	4	5	6	7
5	SUBBAG TU					
	ESELON	1	-	-		
	FUNGSIONAL	-	-	-		
	PELAKSANA	-	-	20		
					21	
	JUMLAH	14	74	91	179	

Gambar 4. 9 Daftar Susunan Personel di Pushansiber

Sumber: Pushansiber KEMHAN RI

Dari faktor-faktor kendala yang dimiliki oleh Pushansiber, instansi tersebut dapat melakukan kerja sama, mengikuti kegiatan seminar dan lain-lain untuk dapat menerapkan dan mengembangkan ilmu dan pengalaman yang dimiliki agar dapat melakukan tahapan pembangunan dan pengembangan atau bahkan dapat menciptakan inovasi terbaru yang mana dapat mengurangi faktor kendala yang sedang di alami. Memberikan pelatihan yang bersifat nasional dan internasional yang mana dapat melakukan kerjasama antara Kementerian Pertahanan dengan Kementerian Luar Negeri yang mengajak bekerjasama dengan negera lain yang kuat dan maju dalam bidang siber. Diberikannya pelatihan dan sertifikasi inernasional untuk dapat memperkuat sistem pertahanan siber.

Peneliti juga mendapatkan data mengenai *hardware, software*, infrastruktur, *firmware* yang mana telah di konfirmasi oleh Bapak Rudy Wahyudi yaitu kondisi nya sekitar 70% yang masih berfungsi dengan baik baik dari sisi kondisi perangakt, namun apabila dilihat dari sisi efektivitas perangakat tersebut sudah sangat berumur dan perlu di ganti dengan perangkat yang mengikuti perkembangan zaman. Dari sektor tersebut yang perlu dimiliki yang mana dapat mengikuti perkembangan *cyber* seperti *hardware, software* untuk dapat melakukan *monitoring* perangkat maupun jaringan dan pengamanan jaringan.

4.3.2 Strategi Pertahanan Siber Indonesia Di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia Dalam Meningkatkan Kapabilitas Pada Sistem Siber

Strategi dari Pusat Pertahanan Siber diperoleh peneliti dengan melakukan wawancara bersama Bapak Irfan Mountini, S. Kom , Bapak Rudy Wahyudi, S. Kom., M. Han dan Bapak Eko Joko Murwanto, S. Kom., M.Si serta beberapa wawancara yang menggunakan *Zoom* yang mengingat kondisi pandemi *covid-19* pada saat ini dengan Bapak Dr. Ir. Achmad Farid W, M dan Bapak Prof. Dr. Ir. Richardus Eko Indrajit M. Sc., MBA., Mphil. MA. Hasil dari wawancara telah menunjukkan pada

narasumber yang mengetahui dalam membangun sistem siber dan Pushansiber sendiri melihat adanya ancaman siber menjadikan ancaman yang serius. Hal tersebut dapat terlihat sebagaimana telah di tetapkan secara khsusu mengenai dalam membangun sistem siber. Adapun tabel untuk penerapan strategi Pushansiber dalam meningkatkan kapabilitas sistem siber dapat dilihat sebagai berikut.

Tabel 4. 1 Penerapan Strategi Pushansiber dalam Meningkatkan Kapabilitas Sistem Siber

Informan	Sumber Daya Manusia	*Hardware*	*Software*	Infrastruktur	*Firmware*	Anggaran	Instansi
Bapak Irfan Mountini, S. Kom , Bapak Rudy Wahyudi, S. Kom., M. Han dan Bapak Eko Joko Murwanto, S. Kom., M.Si	Melakukan pelatihan,pendidikan, mengikuti sertifiasi internasional, dan melakukan dinas kerja	Membeli perangkat yang baru, melakukan *maintenance*	Ingin memiliki *software* yang mutakhir, seperti: Pegasus	Dilengkapi dengan yang baru, melakukan *maintenance*	Dilengkapi dengan yang baru	Anggaran yang ideal untuk dapat membangun sistem siber	PUSHANSIBER
Bapak Dr. Ir. Achmad Farid W, M	Melakukan pelatihan, pendidikan,	Membeli perangkat yang baru	Bekerja sama dengan	Melakukan kerjasama dengan pihak	Melakukan kerjasama dengan	Mengerjakan tugas (*project*)	

	mengikuti sertifiasi internasional, mengisi bagian yang kosong dengan sdm yang memiliki kemampuan IT dan melakukan dinas kerja	apabila perangkat sudah tidak dapat berfungsi, melakukan *maintenance*	BSSN dan Satsiber untuk dapat melakukan inovasi	*vendor,* lembaga atau instansi yang lain.	pihak *vendor,* lembaga atau instansi yang lain.	diluar instansi yang nantinya mendapatkan pendapatan yang nantinya dapat digunakan pada sektor yang lain.	PUSHANSIBER
Bapak Prof. Dr. Ir. Richardus Eko Indrajit M. Sc.,	Melakukan pelatihan, pendidikan yang sifatnya formal dan non-formal,	Membeli perangkat yang baru apabila perangkat	Melakukan *support* pada *endpoint security*	Melakukan kerjasama dengan pihak *vendor,* lembaga atau	Melakukan kerjasama dengan pihak *vendor,*	Untuk anggaran tidak hanya setahun	

MBA., Mphil. MA	mengikuti sertifiasi internasional, mencari sdm yang memiliki kemampuan dan ahli di bidang IT,	sudah tidak dapat berfungsi, melakukan *maintenance*	di *principal* yang nanti nya akan selalu *update*, membeli *renewal signature* jangan hanya setahun saja dll	instansi yang lain.	lembaga atau instansi yang lain.	saja agar dapat *update*	P U S H A N S I B E R

Sumber: diolah peneliti 2022

Berdasarkan tabel diatas, diketahui bahwa untuk dapat meningkatkan kapabilitas sistem siber di Pushansiber dengan menggunakan strategi pertahanan siber baik dari Bapak Irfan Mountini, S. Kom , Bapak Rudy Wahyudi, S. Kom., M. Han dan Bapak Eko Joko Murwanto, S. Kom., M.Si kemudian Bapak Dr. Ir. Achmad Farid W, M dan Bapak Prof. Dr. Ir. Richardus Eko Indrajit M. Sc., MBA., Mphil. MA.

Menurut dari Bapak Bapak Irfan Mountini, Bapak Rudy Wahyudi, dan Bapak Eko Joko Murwanto dalam penerapan pembangunan sistem siber harus didukung oleh anggaran. Apabila anggaran belum dimiliki, maka penerapan strategis belum dapat berjalan sesuai dengan perencanaan. Dengan memanfaatkan dari sektor sdm nya saja belum cukup untuk dapat meningkatkan kapabilitas sistem siber di Pushansiber. Sedangkan menurut Bapak Dr. Ir. Achmad Farid W, M dan Bapak Prof. Dr. Ir. Richardus Eko Indrajit M. Sc., MBA., Mphil. MA memiliki pendapat yang sama dalam penerapan pembangunan sistem siber dengan melakukan pengembangan dan lebih menggodok atau menekankan pada sumber daya manusia nya agar nantinya dapat menghasilkan dan menciptakan sumber daya manusia yang siap, ahli dan inovatif. Dari upaya tersebut, sumber daya manusia nya dapat mengerjakan pekerjaan tambahan diluar instansi yang tidak hanya mengandalkan anggaran dari pemerintah, agar nanti nya dapat mendapatkan penghasilan untuk dapat meningkatkan kapabilitas sistem siber.

Namun sampai saat ini semua perencanaan strategi pertahanan siber menurut dari beberapa informan belum mampu untuk dapat meningkatkan kapablitas pada sistem siber. Di Pushansiber hanya melakukan pengembangan pada sektor sumber daya manusia nya saja. Untuk dapat menunjang kemampuan di bidang IT yang masih belum maksimal dan belum merata. Ditambah dengan adanya kondisi pandemi *covid-19* pada saat ini, semua kegiatan pekerjaan dapat dilakukan dirumah (*work from* home) dan dibatasi karena sesuai dengan intruksi dari pemerintah. Maka

dari itu sumber daya manusia yang dimiliki oleh Pushansiber masih lemah dan pertahanan siber belum siap.

Peneliti juga melakukan kajian mengenai dokumen-dokumen terkait yang diantaranya Pushansiber melakukan diskusi, kerja sama dengan negara lain, mengikuti seminar untuk meningkatkan kualitas, kemampuan dan keahlian pada sektor sumber daya manusia nya.

Pada Gambar 4.10 di bawah ini Kapushansiber Bainstrahan Kemhan yaitu Marma TNI Raja H Manalu dan Kolonel Lek Devis Lebo dan dari satuan kerja Satsiber TNI yaitu Kolonel Chb Tofik Tofana dan Letnan Kolonel Muhammad Ali Agus pada kegiatan *Cyber Bootcamp* di *Australia National University* (ANU). Dalam kegiatan ini telah menjelaskan bagaimana pendekatan pemerintah Australia dalam penanganan keamanan siber, kemudian profil, misi dan keterlibatan dari *Australia Cyber Security Centre* (ACSC) di lingkungan nasional hingga internasional, dan memperkenalkan Pusat Keamanan Siber dan memberikan informasi. Dalam giat tersebut memberikan pengalaman, ilmu dan meningkatkan motivasi dalam pengembangan sumber daya manusia.

Gambar 4. 10 Kunjungan Kapushansiber Di Pusat Keamanan Siber Australia.

Sumber: Kementerian Pertahanan Republik Indonesia (2019)

Gambar 4. 11 Pushansiber Dan Kedutaan Inggris Kembali Lanjutkan Diskusi Kerja sama *Cyber Security*

Sumber: Kementerian Pertahanan Republik Indonesia (2019)

Pada Gambar 4.11 adalah kegiatan yang dilakukan oleh Pushansiber pertemuan dengan Kedutaan Inggris yang melanjutkan perbincangan dengan *Systems Applied Intelligence* (BAEs-AI) yang merupakan perusahaan pada sektor pertahanan, keamanan dan kedirgantaraan multinasional di London, Inggirs yang mana lingkup operasi ke seluruh dunia. Pada pertemuan ini juga dari pihak terkait telah memberikan solusi dalam membangun *Advance Security Operation Center* (ASOC), pelatihan pada sdm, memberikan saran rekomendasi dalam penggunaan peralatan atau teknologi yang dapat menunjang kerja dari Pushansiber.

4.4 Hasil Analisis Data

Analisis data yang dipakai untuk melakukan penelitian merupakan penggunaan dari teori Milles dan Huberman. Dari teknis analisis data mencakup beberapa cara dalam pengumpulan data (*data collection*), kondensasi data (*data condentation*), penyajian data (*data display*), kesimpulan atau verifikasi (*conclusion drawing/verification*) (Miles, Huberman, & Saladana, 2014). Pengumpulan data sudah dijelaskan pada sub bab 4.2 mengenai adanya pengumpulan data. Kemudian kondensasi data dilakukan menggunakan cara memilih dari hasil naskah wawancara yang telah disesuaikan dengan tujuan dalam penelitian guna mengetahui

dan memahami strategi pertahanan siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia.

Fakta yang telah diambil dari data yang sudah diuji pada validitasinya, kemudian dilakukan kondensasi yang menjadi data strategi pertahanan siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia. Selanjutnya pada tingkat analisis data peneliti yang nanti nya melakukan penyajian data. Data yang sudah dikondensasi tepat dan cocok pada strategi pertahanan siber Indonesia di Pusat Pertahanan Siber disajikan dengan tujuan untuk merangkum akses peneliti dalam menyimpulkan yang sesuai dengan data yang di dapat pada saat melakukan penelitian. Berikut dibawah ini merupakan data yang disajikan setelah dikondensasi.

4.4.1 Faktor-Faktor Kendala Dalam Membangun Sistem Siber Guna Menghadapi Ancaman Siber

Pada Pushansiber memiliki faktor-faktor kendala yang dapat menghambat dan mengganggu dalam membangun sistem siber. Hal ini sangat mengkhawatirkan akibat adanya ganguan seperti serangan dan ancaman yang dapat memberikan dampak seperti membahayakan pertahanan dengan lingkup kedaulatan negara, keutuhan, keselamatan dan keamanan Indonesia. Pushansiber dalam hal ini memiliki faktor terbesar adalah pada sektor anggaran. Apabila anggaran belum memenuhi atau belum ada, untuk dapat menjalankan perencanaan pembangunan sistem siber menjadi terhambat dan kualitas dari Pushansiber menjadi menurun. Dengan kondisi pandemi *covid-19*, pemerintah memberikan perhatian dan penanganan khusus di bidang kesehatan. Akhirnya pemerintah melakukan pemotongan anggaran guna pemenuhan kebutuhan pada sektor kesehatan. Ini dapat menciptakan kondisi pada Pushansiber semakin menurun dan mengkahawatirkan.

Kemudian diikuti dengan keterbatasan pada jumlah dan kemampuan sumber daya manusia. Jumlah personel di Pushansiber terbatas, untuk

pemenuhan atau pengisian personel di Pushansiber beberapa masih ada yang belum diisi yang dikarenakan kemampuan dan ilmu mengenai IT masih sedikit. Dalam pemberian sertifikasi internasional dan pendidikan pada Pushansiber masih belum menyeluruh dari level bawah hingga atas, maka manajemen pada sumber daya manusia juga masih belum merata. Ini dapat memberikan pada ilmu pengetahuan dimiliki mengenai IT dan untuk dapat melakukan inovasi secara mandiri masih terbatas yang kemudian motivasi kinerja para pesonel juga akan ikut menurun. Dengan adanya *covid-19*, pemerintah memberikan intruksi untuk dapat melakukan pekerjaan dirumah saja atau *work from home* yang mengakibatkan semua kegiatan menjadi tidak berjalan dan terhambat untuk dapat membangun sistem siber di Pushansiber.

Pada *hardware, software,* infrastruktur dan *firmware* belum adanya pembangunan dan pengembangan kembali dan masih memakai alat yang ada di Pushansiber. Apabila Pushansiber memiliki keterbatasan pada hal tersebut, maka dari sektor sdm nya dapat membantu, melakukan inovasi dan mencari jalan agar terus dapat mengerjakan tugas pokok dari Pushansiber. Namun dari sisi sdm, *hardware, software,* infrastruktur, *firmware* dan *budgeting* belum memenuhi ideal dalam membangun sistem pertahanan siber. Kondisi yang dialami oleh Pushansiber menjadi sangat rawan dan rentan terhadap adanya serangan dan ancaman siber.

4.4.2 Strategi Pertahanan Siber Indonesia Di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia Dalam Meningkatkan Kapabilitas Pada Sistem Siber

Adapaun *Ends* (Tujuan) strategi pada Pushansiber melakukan pembelajaran ulang dari buku nya seperti apa, beli alatnya seperti apa, menghubungi kepada siapa untuk dapat membeli alatnya, bagaimana dari sumber daya manusia nya ada atau tidak, apakah manusianya siap tidak untuk mempelajari dan diberikan pelatihan mengenai IT. Visi dari Pushansiber harus dilihat terlebih dahulu untuk menjadikan rumusan jangka

panjang yang kemudian melakukan pengukuran dengan menggunakan IKU (Index Kinerja Unit) yang mana ini menyangkut dalam pencapaian pada jangka panjang. Pushansiber menggunakan strategi untuk dapat meningkatkan kapabilitas sistem siber yang membutuhkan waktu. Kemudian Pushansiber juga telah membuat dan memasuki pada rencana strategi (renstra) dari tahun 2020-2024. Namun rencana strategi yang sudah dibuat belum dapat di program kan yang dikarenakan memiliki faktor kendala nya. Upaya yang dilakukan oleh Pushan siber dalam meningkatkan kapabilitas dengan mengirimkan personel untuk mengikuti pelatihan, seminar, diskusi, dan memberikan sertifikasi internasional untuk sumber daya manusia. Pushansiber juga mengikuti dan mengahadiri undangan dari negara luar seperti Australia dan Inggris guna membangun sistem siber yang baik. Ketika Badiklat mengadakan pelatihan, personel Pushansiber turut ikut pada kegiatan tersebut.

Adapaun *Ways* (Cara) strategi pada Pushansiber dimana dari infrastruktur harus jalan, dapat dioperasikan, sumber daya manusia nya terpenuhi dan yang pastinya harus memiliki program untuk dijalankan. Maka untuk dapat meningkatkan kapabilitas sistem siber harus memiliki program untuk dijalankan. Instruksi nya sudah ada dan rencana strategis di tahun 2020 sampai 2024 mengenai prioritas dalam pembangunan pertahanan siber. Ini bentuk arahan dari pemimpin di Kementerian Pertahanan dengan adanya instruksi tersebut dan harus di optimalkan. Pemerintah membuat dan menerapkan langsung dalam mengharmoniskan regulasi mengenai siber di Indonesia agar dapat melakukan kerja sama pada tiap lembaga seperti BSSN atau yang lain yang memiliki kemampuan pada bidang IT dan kerja sama pada industri untuk dapat meningkatkan dan memperkuat pertahanan Indonesia. Kemudian membuat alur ekosistem siber, melakukan pemetaan pada ancaman dan serangan, membuat perubahan pada pola pikir yang menjadikan pembangunan dan pengembangan sistem siber, melakukan perubahan dari kultur dari lintas generasi, kebiasaan dan literasinya. Kemudian memberikan pelatihan,

pendidikan dan lain-lain untuk dapat meningkatkan kualitas pada sektor manusia. Membeli teknologi yang baru agar dapat melakukan tugas dengan baik. Kemudian melakukan perekrutan dari masyarakat yang memang memiliki kemampuan pada IT agar dapat di pekerjakan sebagai PNS dan merekrut mahasiswa di seluruh Indonesia dari berbagai perguruan tinggi yang memiliki kepintaran dan ahli di bidang IT agar dapat di pekerjakan di Pushansiber dan dijadikan Pegawai Negeri Sipil (PNS).

Adapaun *Means* (Sarana Prasarana) apabila melihat dari Permenhan No. 82 Tahun 2014 mengenai penangkalan, penindakan dan pemulihan harus memiliki ruangan *monitoring* untuk dapat melihat ada apa saja, untuk dapat mendukung kegiatan yang lain harus ada lab-lab yang lain juga. strategi pada Pushansiber dalam mendukung sistem siber harus memiliki *data center, monitoring, lab,* perangkat-perangkat yang mutakhir kemudian pada sistem pendukungnya juga harus diikuti, seperti: *supply* lisrtriknya, sirkulasi udara nya dan lain-lain. Idealnya server pada pertahanan seharusnya berada di Pushansiber, karena tugas dari Pushansiber untuk dapat mengamankan. Mereka hanya melakukan via *remote* saja, namun pada fakta nya belum direalisasikan.

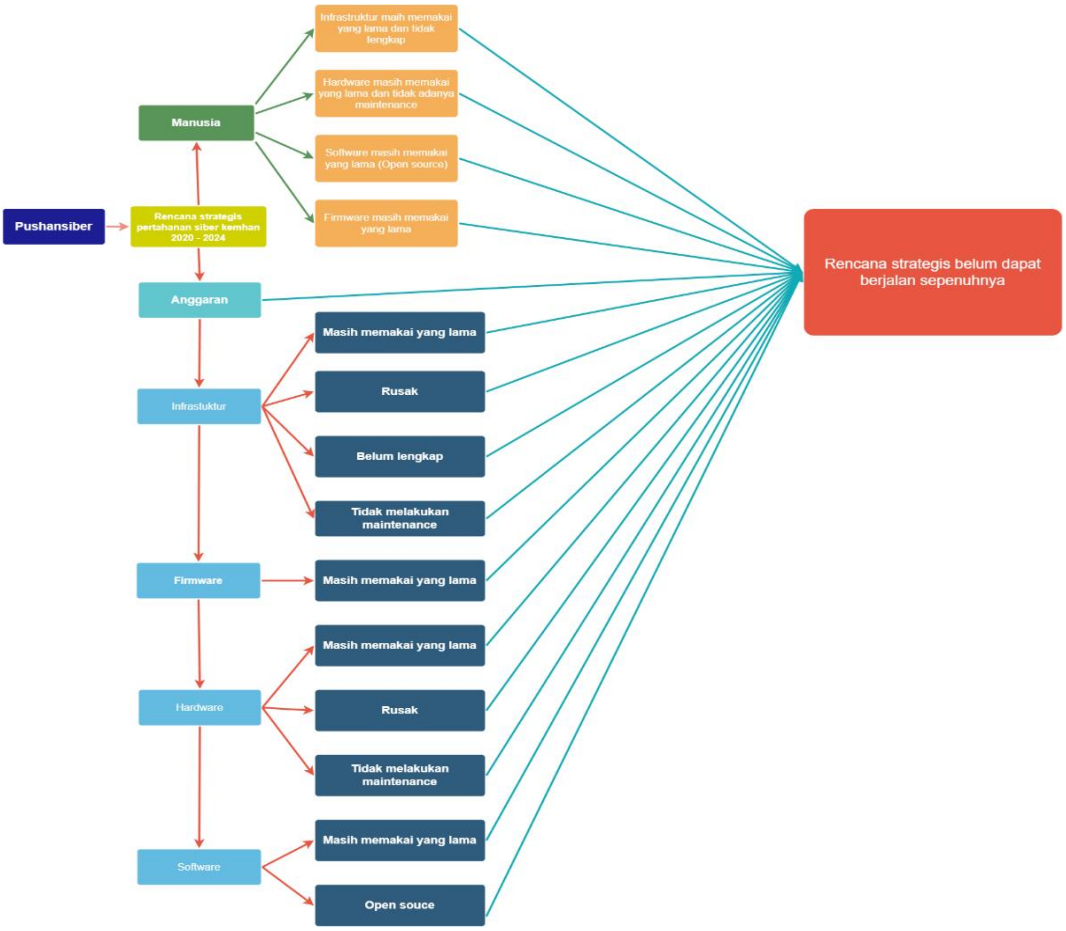
4.5 Interpretasi Data

Dalam Interpretasi data, peneliti melakukan menginterpretasikan data yang telah diyakini adanya keabsahannya. Kesimpulan awal yang sudah didapat dari analisis data dengan menggunakan proses pengumpulan data, kondensasi, penarikan kesimpulan dan penyajian data yang menghubungkan satu sama lain yang nantinya dapat menjawab dari pertanyaan penelitian yang sudah ditentukan.

4.5.1 Faktor-Faktor Kendala Dalam Membangun Sistem Siber Guna Menghadapi Ancaman Siber

Faktor-faktor kendala dalam membangun sistem siber di Pushansiber membuat penurunan pada kualitas dan kemampuan kerja yang harus ditangani cepat dan dianggap serius. Faktor kendala yang terbesar pada Pushansiber adalah anggaran. Pushansiber belum memiliki atau terpenuhi dari segi anggaran khusus untuk membangun sistem siber.

Teori dari *Sixware Network Security Framework* (SWNSF) belum dapat dipakai dalam membangun sistem siber di Pushansiber yang dikarenakan letak posisi anggaran lebih penting, yang kemudian diikuti oleh faktor manusia (*brainware*), perangkat keras (hardware), perangkat lunak (*software*), infrastruktur (*infrastruktur*), *firmware.* Apabila anggaran belum dimiliki atau terpenuhi, maka perencanaan strategi yang sudah di buat belum dapat berjalan dengan baik. Kemudian pada situasi atau kondisi pandemi *covid-19* pada saat ini, pemerintah lebih memberikan perhatian pada sektor kesehatan, yang akhirnya membuat anggaran khusus untuk membangun sistem siber dipotong oleh pemerintah dan semua kegiatan aktivitas menjadi di batasi dan terhambat.



Gambar 4. 12 Faktor-faktor kendala dalam membangun sistem siber di Pushansiber

Sumber: diolah peneliti 2022

4.5.2 Strategi Pertahanan Siber Indonesia Di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia Dalam Meningkatkan Kapabilitas Pada Sistem Siber

A. Teori Ilmu Pertahanan

Pertahanan negara memiliki arti yang sangat penting bagi Indonesia untuk dapat merancang strategi pertahanan negara yang memakai seluruh kekuatan dan kemampuan dari sektor militer maupun non militer secara terpadu dan menyeluruh (Kemenhan, 2015). Pushansiber selalu berupaya untuk kuat agar nantinya dapat menjaga dan melindungi terhadap adanya serangan dan ancaman

siber. Dikarenakan banyak dokumen negara yang seharusnya di lindungi dan di jaga yang menjadi pusat incaran dan kerawanan yang dilakukan oleh penjahat siber.

Pada buku ilmu pertahanan yang dikatakan oleh Makmur Supriyatno (2014) memasukan strategi sebagai unsur penerapan dari berbagai ilmu dan digunakan sebagai alat (kekuatan dalam bersenjata / pasukan) yang mana masuk kedalam *means*, adanya metode atau langkah yang masuk (*ways),* yang kemudian merujuk pada tujuan (*ends*) guna untuk mengurangi adanya ancaman dan siap untuk mengalahkan. Ini dapat menjadi sebuah strategi pertahanan siber Indonesia dalam membangun sistem siber. Ketika melihat teknologi informasi menjadi hal yang vital dan bentuk perubahan baru. Pada kondisi saat ini perang informasi dapat menjadi ancaman siber di Indonesia. Maka dari itu informasi menjadi insturmen yang dapat menciptakan peperangan.

Menurut Makmur Supriyatno (2014) menjelaskan di dalam bukunya yang mengenai perumusan pertahanan negara yang memerlukan strategi dalam memanajemen pertahanan, maka yang harus di perhatikan yakni adanya manajemen dalam sumber daya manusia pertahanan yang didalam nya memiliki potensi SDM pada pertahanan yang kini masih pada tahap pengaturan lebih lanjut pada peraturan perundangan, yang akhirnya manajemen SDM pada saat ini masih dalam proses pengembangan dan peningkatkan guna menuju kedaulatan siber nasional. Kemudian adanya manajemen dalam anggaran dan keungan yang pada dasarnya anggaran pertahanan memang seharusnya keluar angka yang belandaskan dari situasi ancaman yang nantinya akan dihadapi. Ini menjadikan faktor penting dalam menuju kedaulatan siber nasional demi menjaga dan melindungi segenap bangsa dan negara. Lalu adanya manajemen dalam industri dan teknologi pertahanan yang terdapat Komite Kebijakan Indsutri Pertahanan (KKIP) yang telah sesuai dengan

Undang-Undang Nomor 16 Tahun 2012 mengenai Industri Pertahanan yang sesuai dengan Pasal 18 UU. KKIP juga memiliki tugas utama yaitu melakukan pengkoordinasian dalam kebijakan nasional pada perencanaan, perumusan, pelaksanaan, pengendalian, sinkronisasi dan evaluasi pada Industri Pertahanan di Indonesia. Kemudian adanya manajemen informasi, intelijen dan pengetahuan pertahanan yang harus dikelola dengan sebaik mungkin, dikarenakan informasi, intelijen dan pengetahuan pertahanan adalah mata dan telinga dan sekaligus menjadi sumber bahan pengambilan keputusan pada kenegaraan terutama di sektor pertahanan. Munculnya kerawanan pada sistem pertahanan siber yang dapat mengganggu kedaulatan, keutuhan dan keselamatan bangsa, perlu adanya strategi mitigasi yang efektif. Karena tidak adanya negara aman dari serangan dan ancaman siber.

B. Teori Strategi

Strategi Pushansiber dalam meningkatkan kapabilitas sistem siber menggunakan acuan dari Kementerian Pertahanan yang memiliki visi dan misi yang terarah, menyeluruh dan terpadu yang dikarenakan melihat dari ideologi bangsa yang berlandaskan kehidupan bernegara pada Pancasila dan UUD 1945 dalam konsep pertahanan siber negara. Dari doktrin pertahanan negara juga telah di pakai sebagai tujuan dan falsafah negara. Melakukan pemetaan ancaman militer dan non militer yang dapat mengganggu pertahanan suatu negara. Strategi ini sudah dilakukan oleh pihak Pushansiber dalam *domain Ends*, namun ternyata masih dirasa belum kuat dan siap dalam meningkatkan kapabilitas sistem siber. Pada *domain Ways* mempunyai sejumlah komponen yang penting seperti adanya strategi dalam penanganan ancaman yang dapat mengidentifikasi melalui *soft power , hard power*, maupun *smart power*, dan mempunyai jangka yang panjang , jangka pendek dan jangka menengah, strategi pengelolaan sumber daya pertahanan yang

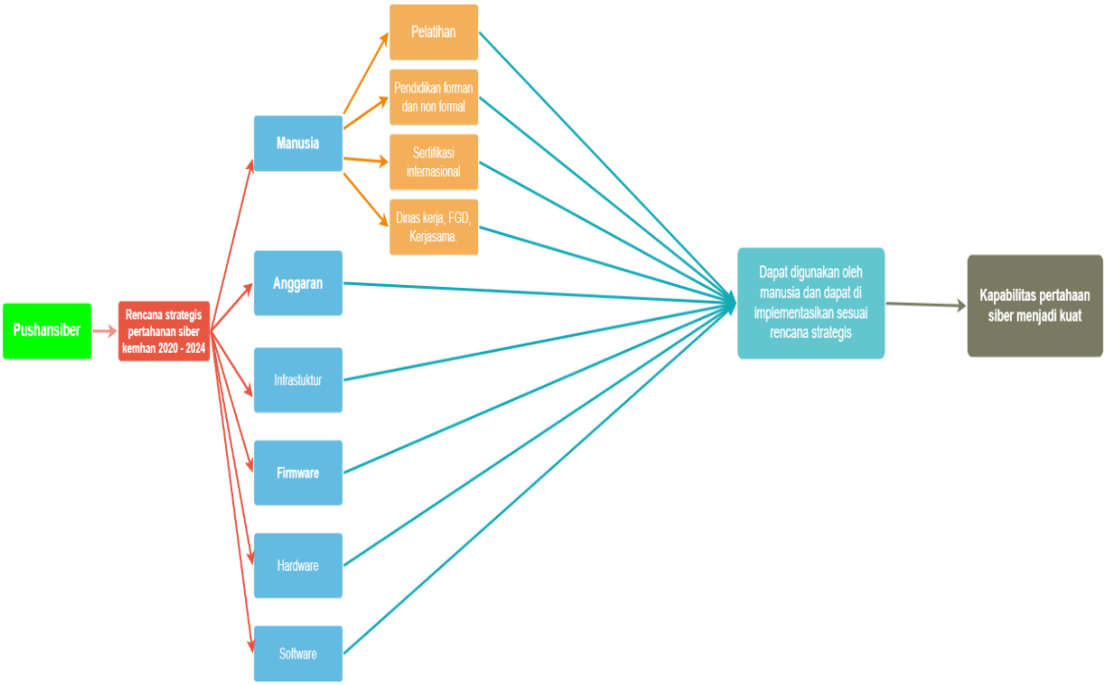
berupa siklus manajerial yaitu pengadaan guna untuk dapat menjadi sebuah program pemerintah. Dan *domain* terakhir adalah *Means* terdapat adanya komponen pertahanan yang memiliki komponen utama, cadangan, dan komponen pendukung untuk dapat membela sebuah negara, yang menjadikan semangat seluruh warga negara dalam menciptakan dan menumbuhkan nasionalisme yang tinggi pada sumber daya manusia, pada kondisi negara yang sangat strategis seperti indonesia dengan memiliki banyaknya sumber kekayaan alam dan budaya menjadikan unsur kekuatan nasional yang terkandung dalam fisik maupun aset.

C. Teori *Sixware Network Security Framework*

Strategi Pertahanan Siber di Pushansiber dalam meningkatkan kapabilitas pada sistem siber menggunakan acuan dalam Permenhan No. 82 Tahun 2014 sebagai pedoman pertahanan siber dalam upaya membangun sistem siber dan pencegahan dari ancaman siber. Dalam penguatan kapabilitas sistem siber, harus ada dukungan dalam pemenuhan sumber daya manusia, perangkat keras, perangkat keras, infrastruktur dan firmware agar pertahanan siber Indonesia menjadi siap terhadap adanya ancaman dan serangan.

Ketika melihat kembali dengan pernyataan konsep yang di buat oleh Rudy Gultom (2018) mengenai adanya 6 dasar dalam membangun sistem siber, seperti: Faktor manusia (*brainware*), perangkat keras (hardware), perangkat lunak (*software*), infrastruktur (*infrastruktur*), *firmware* dan anggaran (*budgeting*). Namun di Pushansiber strategi dalam meningkatkan kapabilitas sistem siber yaitu: anggaran (*budgeting*), faktor manusia (*brainware*), perangkat keras (hardware), perangkat lunak (*software*), infrastruktur (*infrastruktur*), *firmware.*

Strategi yang dipakai Pushansiber dalam meningkatkan kapabilitas sistem siber dengan teori *Sixware Network Security Framework* (SWNSF) memiliki perberbedaan. Menurut Pushansiber dalam meningkatkan kapabilitas sistem siber anggaran menjadi sesuatu hal yang terpenting. Kemudian setelah itu beralih pada sumber daya manusia nya yang harus diberikan pelatihan, pendidikan yang sifatnya formal dan non-formal, sertifikasi internasional dan pengiriman personel dalam giat dinas kerja yang nanti nya akan meningkatkan pada kemampuan, ilmu, motivasi, pengalaman dan dapat menghasilkan inovasi dalam tujuan membangun sistem sibernya. Lalu diikuti dengan membeli dan melengkapi perangkat-perangkat terbaru, dan melakukan *maintenance* pada perangkat yang baru dan lama.



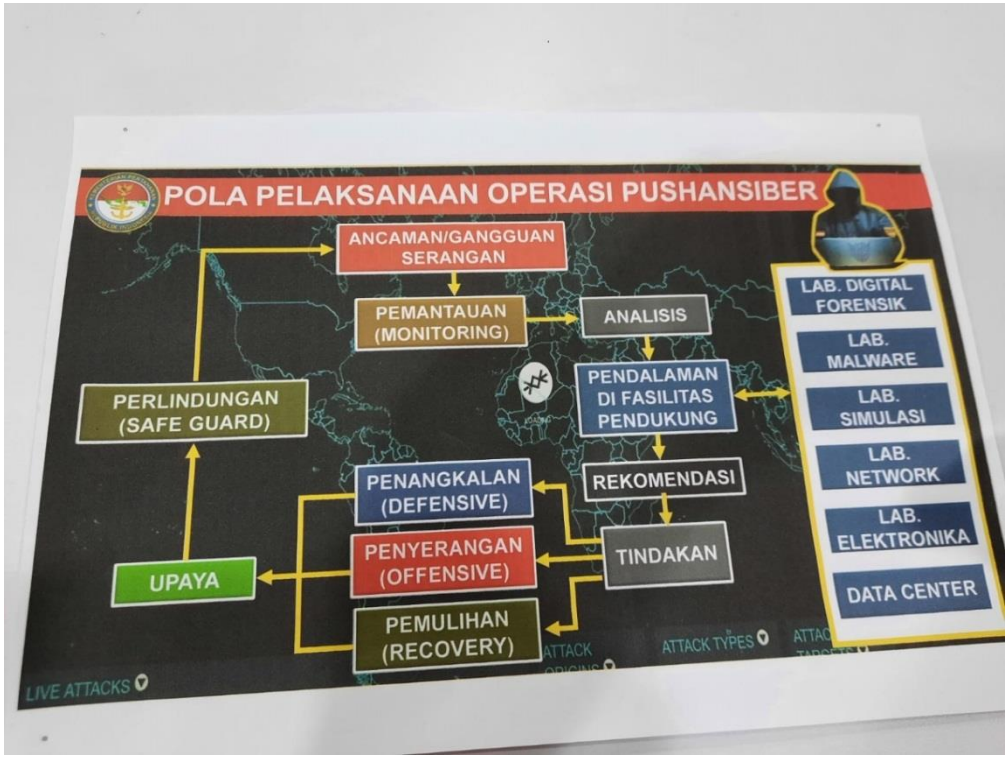
Gambar 4. 13 Strategi Pertahanan Sibebr di Pushansiber Dalam Meningkatkan Kapabilitas Sistem Siber

Sumber: diolah peneliti 2022

Penjelasan mengenai Strategi Pushansiber dalam meningkatkan kapabilitas sistem siber diatas, pada saat ini belum dapat terlaksana dengan baik yang dikarenakan adanya faktor kendala pada Pushansiber. Ini menjadi permasalahan yang serius dan seharusnya pemerintah memberikan perhatian dan dukungan penuh terhadap pentingnya pertahanan siber di Kementerian Pertahanan khususnya di Pushansiber.

D. Teori keamanan sistem

Teori keamanan sistem sangat berperan penting dalam meningkatkan kapabilitas sistem siber di Pushansiber dan bahkan dapat melindungi dan menjaga jalannya suatu sistem yang terhubung satu sama lainnya. yang dimana *firewall* mempunyai keunggulan seperti *packet-filtering firewall, NAT Firewall, Circuit-Level Firewall* dan *Proxy Firewall.* Dan pushansiber sudah membuat pola pelaksanaan operasi pushansiber, seperti gambar gambar dibawah. :



Gambar 4. 14 Pola pelaksanaan operasi Pushansiber

Sumber: Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia

4.6 Pembahasan

4.6.1 Faktor-Faktor Kendala Dalam Membangun Sistem Siber Guna Menghadapi Ancaman Siber

Pada faktor-faktor kendala dalam membangun sistem siber guna menghadapi ancaman siber merupakan permasalahan yang dihadapi dan dimiliki oleh Pushansiber. Disini terlihat bahwa Pushansiber belum mampu membangun sistem siber yang dikarenakan belum adanya pemenuhan pada keenam dasar dalam membangun sistem siber, seperti: faktor manusia *brainware*), perangkat keras (hardware), perangkat lunak (*software*), infrastruktur (*infrastruktur*), *firmware* dan anggaran (*budgeting*).

Pushansiber menitik beratkan faktor kendala yang utama pada sektor anggaran untuk dapat menyokong dan pemenuhan dari ke 6 dasar dalam membangun sistem siber. Padahal rencana strategis dalam anggaran sudah dirancang untuk tahun 2020-2024, namun pada kenyataannya masih belum ada anggaran yang khusus untuk sistem siber. Pemerintah sedang memberikan perhatian khusus pada sektor kesehatan di situasi pandemi seperti ini yang menyebabkan anggaran tersebut dipotong untuk di arahkan pada sektor kesehatan. Dengan adanya keterbatasan dalam anggaran, maka Pushansiber memanfaatkan dari sumber daya manusia nya sepeti dalam memberikan pelatihan, diikut sertakan dalam sertifikasi internasional, pengiriman personel untuk melakukan dinas kerja yang nanti nya dapat menghasilkan sdm yang siap dan memiliki kemampuan. Pada situasi pandemi *covid-19* ini memberikan pembatasan pada kegiatan kerja yang mengakibatkan semua kegiatan menjadi terhambat dan dibatasi.

Namun dalam hal ini Pushansiber juga belum mampu memanfaatkan sdm secara menyeluruh dengan adanya keterbatasan dalam kemampuan, ilmu, pengalaman dan biaya. Pada sektor perangkat keras (hardware), perangkat lunak (*software*), infrastruktur (*infrastruktur*), *firmware* juga masih belum dilakukannya pembangunan, pengembangan dan pengadaan. Semua perangkat masih menggunakan perangkat yang lama, terdapatnya

beberapa perangkat sudah tidak bisa dimanfaatkan, masih menggunakan *open source,* dan bahkan sering belum melakukan *maintenance* dikarenakan dari beberapa personel masih ada yang belum memahami dalam bagaimana cara memanfaatkan perangkat tersebut.

Sebelumnya Pushansiber fokus pada 3 elemen yaitu *people, technology* dan *process,* namun ketika anggaran menjadi faktor kendala utama, maka Pushansiber merubah anggaran menjadi posisi no. 1. Dengan terpenuhi nya anggaran, maka *people, technology* dan *process* nantinya akan terpenuhi. Maka peneliti menemukan bahwa teori dari *Sixware Network Security Framework* (SWNSF) belum dapat digunakan dalam membangun sistem siber di Pushansiber yang dikarenakan letak anggaran menjadi lebih penting, yang kemudian diikuti oleh faktor manusia (*brainware*), perangkat keras (hardware), perangkat lunak (*software*), infrastruktur (*infrastruktur*), *firmware.*

Seharusnya Pushansiber lebih memperdalam pada sektor sdmnya untuk dapat menghasilkan dan menciptakan sdm yang kuat, siap, dan memiliki pengalaman di bidang IT. Apabila dari sektor sdm sudah mulai terpenuhi, maka dari sektor perangkat keras (hardware), perangkat lunak (*software*), infrastruktur (*infrastruktur*), *firmware* dan anggaran akan terpenuhi. Untuk dapat melakukan hal tersebut dapat dilakukan seperti: memberikan pelatihan kepada sdm nya dari tingkat bawah sampai atas, agar manajemen kualitasnya merata. Kemudian memberikan kesempatan untuk melakukan pendidikan dari yang sifatnya normal dan non-formal, kemudian diberikannya sertifikasi secara menyeluruh pada semua personelnya. Lalu mengirimkan personelnya untuk melakukan dinas kerja yang nantinya mendapatkan ilmu dan pengalaman di bidang IT. Mengisi bagian bidang kerja dengan orang-orang yang memiliki kemampuan dan kompeten di bidang IT. Mempererat dan meningkatkan jalinan hubungan kerjasama dengan berbagai instansi, vendor atau dari negara luar untuk dapat membangun sistem sibernya. Merekrut mahasiswa yang cerdas di bidang IT dari tiap-tiap Universitas. Karena dari orang organik nya belum

siap, maka lebih baik merekrut sdm nya berasal dari luar yang nantinya dapat di PNS kan. Pemerintah juga harus memberikan perhatian khusus dan serius dalam membangun sistem pertahanan siber seperti membuat regulasi yang berhubungan langsung dengan siber dan dapat di selaraskan untuk dapat memperkuat satu sama lainnya dan dalam penyusunan regulasi mengenai pertahanan siber juga seharusnya dapat disesuaikan dengan kondisi perkembangan teknologi yang cepat dan adanya dinamika lingkungan yang strategis.

4.6.2 Strategi Pertahanan Siber Indonesia Di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia Dalam Meningkatkan Kapabilitas Pada Sistem Siber

Berdasarkan hasil penelitian dan analisis yang sudah dilakukan, menghasilkan bahwa strategi pertahanan siber Indonesia di Pushansiber Kemhan RI dalam meningkatkan kapabilitas pada sistem siber masih belum berjalan dengan maksimal yang dikarenakan memiliki faktor-faktor kendala. Peningkatan serangan dan ancaman yang diberikan oleh penjahat siber dengan memanfaatkan kelemahan pada IT dan teknologi. Hal ini belum sesuai dengan teori Liddell Hart (1967), yang menyebutkan bahwa untuk strategi bentuk dalam penentuan untuk mencapai tujuan akhir (*ends),* yang kemudian strategi dipakai untuk dapat mencapai hasil akhir (*ways*) dan yang terakhir adanya sarana dan prasarana guna mencapai tujuan (*means*), antara lain:

a. Tujuan (*Ends*)

   Pushansiber memiliki visi, misi dan tujuan nasional yang sesuai dengan undang-undang yang membahas mengenai ideologi bangsa Indonesia yang menyangkut kehidupan berbangsa dan bernegara, seperti Pancasila dan UUD 1945. Kemudian adanya Permenhan No. 82 Tahun 2014 sebagai pedoman pertahanan siber. Memberikan informasi mengenai adanya ancaman dan serangan siber yang dapat mengganggu keselamatan dan keamanan pertahanan Indonesia.

Namun masyarakat Indonesia masih belum mengetahui atau awam dan minimnya kesadaran dengan adanya jenis-jenis gangguan yang dapat menimpa pertahanan siber di Indonesia. Hal inilah yang dimanfaatkan oleh para penjahat siber untuk dapat menyerang dan memberikan ancaman. Dan memperkuat dan siap pada lini sistem pertahanan siber Indonesia terhadap rentannya ancaman dan serangan yang dimanfaatkan oleh para penjahat siber.

b. Cara (*Ways*)

Membuat alur ekosistem pada sektor siber, membuat pemetaan terhadap adanya ancaman dan serangan, membuat perubahan pada pola pikir yang menjadikan pembangunan dan pengembangan sistem siber kembali, memberikan pemahaman mengenai apa saja kerentanan yang nantinya kedepannya, kemudian melakukan perubahan dari kultur dari lintas generasi, kebiasaan dan literasinya. Lalu memberikan pelatihan, pendidikan, merekrut mahasiswa di seluruh Indonesia dari berbagai perguruan tinggi yang memiliki kecerdasan dan kemampuan di bidang IT agar dapat di pekerjakan di Pushansiber dan dijadikan Pegawai Negeri Sipil (PNS) atau bahkan dapat melakukan perekrutan dari masyarakat yang memang bukan organik atau anggota TNI tetapi memiliki kemampuan pada IT agar dapat di pekerjakan sebagai PNS dan maka dari itu pemerintah harus merubah peraturan agar sumber daya manusia yang memiliki kemampuan khusus di bidang IT dapat di pekerjakan sebagai PNS, guna dapat meningkatkan kualitas pada sektor manusia. Melakukan pemeliharaan, melengkapi dan membeli perangkat keras, lunak, infrastruktur dan *firmware* yang baru agar dapat melakukan tugas dengan baik.

Pushansiber telah membuat perencanaan strategis mulai dari yang sifatnya jangka panjang, menengah dan pendek. Lalu Membuat rancangan strategi untuk melakukan penanganan apabila adanya ancaman. Kemudian membuat adanya pembangunan, pengembangan dan pengadaan kembali. Pemerintah memberikan dukungan penuh dan menganggap ini menjadi hal yang serius. Namun sampai saat ini belum melakukan adanya pembangunan, pengembangan dan pengadaan kembali dan menjadikan kondisi pertahaan siber di Indonesia menjadi rawan. Pada saat situasi pandemi *covid*-19, pemerintah lebih fokus pada sektor kesehatan dan ekonomi. Hal inilah yang dimanfaatkan oleh para penjahat siber untuk dapat menyerang dan memberikan ancaman.

c. Sarana dan Prasarana (*Means*)

Sarana dan Prasana menjadi penunjang dan sumber daya yang strategis dimiliki oleh negara. Indonesia juga didukung oleh 3 komponen pertahan, seperti komponen utama, cadangan dan pendukung yang harus diberikan pemahaman IT dan pelatihan di bidang siber untuk menjadikan alat dalam pertahanan negara. Kemudian di sokong dari banyak rakyat Indonesia yang menjadikan Indonesia sebagai sistem pertahanan di Indonesia yang bersifat semesta yang sesuai pada Undang-Undang No 3 Tahun 2002 terkait usaha negara dalam menjaga dan melindungi segenap bangsa Indonesia. Pemerintah membuat program dan menanamkan bela negara yang mana sebagai bentuk dari *soft defense* pada pertahanan negara yang dapat menghasilkan rasa kesadaran akan adanya serangan dan ancaman siber. Namun hal ini belum menyeluruh untuk dapat diterapkan. Seharusnya pemerintah melakukan perekrutan Mahasiswa di bidang IT yang paling pintar dari tiap-tiap universitas untuk dapat mendukung dan meningkatkan kemampuan di bidang siber. Kemudian mendirikan insitusi khusus mengenani *cyber security*.

Kemudian lebih di tingkatkan dalam bekerja sama dengan pihak instansi atau lembaga lainnya dan pada industri alutista guna mendapatkan penambahan dalam potensi kekuatan pertahanan nasional.