OPTIMALISASI KEMAMPUAN LABORATORIUM PENGAMANAN SISTEM DAN JARINGAN (LABPAMSISJAR) DISPAMSANAL GUNA MENGAMANKAN INFRASTRUKTUR INFORMASI VITAL (IIV) DALAM RANGKA MEWUJUDKAN KEAMANAN SIBER TNI ANGKATAN LAUT

Jenius, S.KEL., M.M., C.TIA.[1], DR. Imam Teguh Santoso, S.T., M.Si.[2], Teddy Yulianda Bakri.[3]
Strategi Operasi Laut, Sekolah Staf dan Komando Angkatan Laut, Jakarta Selatan, Indonesia
Email: [1]aerosta@gmail.com, [2]imam_teguh santoso@seskoal.ac.id, [3]rahjaro@gmail.com

ABSTRAK

Laboratorium Pengamanan Sistem dan Jaringan (Labpamsisjar) sebagai satuan kerja unit pelaksana teknis yang berada di bawah naungan Dinas Pengamanan dan Persandian Angkatan Laut (Dspamsanal) mempunyai fungsi pembinaan pengamanan, materiil dan administrasi, terhadap kegiatan yang berkaitan dengan keamanan sistem informasi dan jaringan yang meliputi penelitian, pengujian, penangkalan, eksploitasi, penanggulangan dan perbantuan/ dukungan. Labpamsisjar yang berkedudukan dibawah Dispamsanal belum optimal dalam melaksanakan kegiatan pengamanan Infrastruktur Informasi Vital, karena belum sesuainya pemenuhan personil (SDM) secara kuantitas dan kualitas, belum ada kebijakan resmi terkait validasi organisasi Labpamsisjar, sarana prasarana yang tidak sesuai program kerja. Metode penelitian dalam Taskap ini menggunakan metode deduktif deskriptif analitif, untuk mengidentifikasi dan merumuskan strategi yang akan digunakan. Metode penelitian juga didukung dengan teori-teori yang berkaitan dengan sumber daya manusia, organisasi, sarana prasarana dan literatur terkait keamanan siber, sehingga diharapkan dapat menjadikan Labpamsisjar mempunyai kemampuan yang optimal guna mengamankan Inrastruktur Informasi Vital (IIV) TNI Angkatan Laut. Optimalisasi kemampuan Labpamsisjar Dispamsanal merupakan bentuk komitmen TNI AL dalam mendukung kebijakan pemerintah guna melindungi IIV bidang pertahanan dan sekaligus mendukung strategi keamanan siber nasional dan manajemen krisis siber sehingga memerlukan pembahasan dan pemecahan masalah. Pembahasan dilaksanakan dengan menggunakan landasan pemikiran dihadapkan pada faktor-faktor yang mempengaruhi baik eksternal maupun internal dengan mempertimbangkan peluang dan kendala yang ada agar tercapai kondisi kemampuan Labpamsisjar yang diharapkan. Guna mewujudkan hal ini diperlukan rumusan kebijakan, strategi dan upaya oleh berbagai pihak yaitu Mabes TNI dan Mabes TNI AL serta instansi terkait melalui metode Sosialisasi, Retrukturisasi, Kerjasama, Evaluasi, Inventarisasi, Pengadaan dan Modernisasi. Apabila optimalisasi kemampuan Labpamsisjar Dispamsanal tercapai maka dapat mengaman perlindungan IIV dan keamanan siber di lingkungan TNI Angkatan Laut.

Kata Kunci : Optimalisasi, Personil, Organisasi, Infrastruktur dan *Cybersecurity*

ABSTRACT

The System and Network Security Laboratory (Labpamsisjar) as a work unit of the Technical Implementation Unit under the auspices of the Navy Security and Encryption Service (Dspamsanal) has the function of fostering security, material and administration, on activities related to information system and network security which include research, testing, deterrence, exploitation, countermeasures and assistance / support. Labpamsisjar which is located under Dispamsanal has not been optimal in carrying out Vital Information Infrastructure security activities, because it is not suitable for the fulfillment of personnel (HR) in quantity and quality, there is no official policy related to the validation of the Labpamsisjar organization, infrastructure facilities that are not in accordance with the work program. The research method in Taskap uses deductive descriptive analytical methods, to identify and formulate strategies to be used. The research method is also supported by theories related to human resources, organizations, infrastructure and literature related to cybersecurity, so that it is expected to make Labpamsisjar have optimal capabilities to secure the Vital Information Infrastructure (IIV) of the Indonesian Navy. The optimization of Labpamsisjar Dispamsanal's capability is a form of the Navy's commitment in supporting government policies to protect IIV in the defense sector and at the same time supporting the national cybersecurity strategy and cyber crisis management so that it requires discussion and problem solving. The discussion was carried out using the rationale of being faced with factors that affect both external and internal by considering the opportunities and constraints that exist to achieve the expected condition of Labpamsisjar capabilities. To realize this, it is necessary to formulate policies, strategies, and efforts by various parties, namely TNI Headquarters and Navy Headquarters and related agencies through methods of Socialization, Restructuring, Cooperation, Evaluation, Inventory, Procurement and Modernization. If the optimization of Labpamsisjar Dispamsanal capabilities is achieved, it can secure IIV protection and cybersecurity within the Navy.

Keyword: Optimization, Personnel, Organization, Infrastructure and Cybersecurity

1. PENDAHULUAN

Keamanan siber telah menjadi isu prioritas seluruh negara di dunia semenjak teknologi informasi dan komunikasi dimanfaatkan dalam berbagai aspek kehidupan, baik dalam aspek sosial, ekonomi, hukum, organisasi, kesehatan, pendidikan, budaya, pemerintahan, keamanan, pertahanan, dan lain sebagainya. Menyikapi fenomena tersebut, dalam rangka mewujudkan keamanan siber (*cybersecurity*) di lingkungan TNI Angkatan Laut maka dibutuhkan kemampuan siber yang handal agar mampu menjaga keamanan dan integritas sistem komputer dan jaringan yang digunakan oleh TNI AL. Upaya mewujudkan keamanan siber TNI Angkatan Laut bertujuan untuk melindungi sistem komputer, jaringan, dan sistem basis data yang merupakan bagian penting dari Infrastruktur Informasi Vital (IIV).

Badan Siber dan Sandi Negara (BSSN) menyatakan bahwa keamanan siber pada Infrastruktur Informasi Vital (IIV) nasional harus diamankan, karena apabila terjadi gangguan akan berdampak pada pelayanan publik dan kepentingan umum Serangan siber dapat berasal dari pihak luar maupun serangan dari dalam suatu organisasi dapat berdampak langsung ataupun tidak langsung, dan dampaknya akan dirasakan dalam waktu jangka panjang. Laboratorium Pengamanan Sistem dan Jaringan (Labpamsisjar) diharapkan mampu mewujudkan keamanan siber di lingkungan TNI Angkatan Laut dengan bersinergi dengan satuan siber lainnya di bawah Kementerian Pertahanan, Mabes TNI/ Angkatan, BSSN dan pihak terkait lainnya. Dalam pelaksanaan tugasnya saat ini Labpamsisjar masih diperhadapkan dengan kondisi keterbatasan jumlah kekuatan personil dan tingkat kemampuan sumber daya manusia, khususnya sebagai tenaga professional dibidang siber yang mampu menjawab dan mengahdapi segala bentuk ancaman, gangguan dan tantangan dalam kegiatan operasi *cyber warfare.* Disisi lain Labpamsisjar juga dihadapkan dengan kendala terkait dengan regulasi dan aturan yang dalam pelaksanaan tugasnya belum sepenuhnya sejalan dengan doktrin siber TNI.

Diharapkan Labpamsisjar dapat menjadi cikal bakal dalam berdirinya satuan siber TNI Angkatan Laut yang memiliki kemampuan dalam menyelenggarakan kegiatan siber mulai dari perencanan operasi dan latian, dukungan administrasi dan logistik, pertahanan, pengkalan, penindakan, pemulihan dan perbantuan dalam menerima aduan insiden siber yang terjadi di lingkungan TNI Angkatan Laut. Sedangkan dari segi infrastruktur saat ini, Labpamsisjar berupaya melengkapi diri dengan perangkat siber yang dilakukan secara bertahap. Adapun beberapa perangkat keamanan yang sudah dimiliki Labpamsisjar diantaranya sistem keamanan jaringan (*firewall*), *Security Information and Event Management* (SIEM), *Intelligent Monitoring Analisys* (IMA), *Endpoint protection*, analisa Kedepannya Labpamsisjar diharapkan mampu menjadi komponen utama dalam menjalankan tugas dalam rangka mewujudkan keamanan siber TNI AL yang kompleks dan siap saat

dihadapkan dengan ancaman gangguan dan tantangan *cyber warfare*.

2. METODE PENELITIAN

Metode yang digunakan dalam penulisan ini menggunakan metode deduktif *deskriptif analitik* dengan pendekatan sosiologi yang bersifat empiris. Pendekatan sosiologi didasarkan tinjauan kepustakaan, pengetahuan faktual dan berdasarkan pengalaman penulis dalam penugasan di Labpamsisjar Dispamsanal.

3. HASIL DAN PEMBAHASAN

Awal pembentukan organisasi Labpamsisjar dimulai dari penunjukkan personil TNI AL dari tingkat bintara, pama hingga pamen untuk menjadi calon pengawak siber. Penunjukkan calon pengawak (cawak) siber untuk mengisi kebutuhan organisasi melalui penugasan Bawah Kendali Operasi (BKO) Dispamsanal setelah Labpamsisjar diresmikan pada tahun 2018. Dalam pelaksanaan tugasnya, Kalabpamsisjar bertanggung jawab kepada Kadispamsanal dibawah supervisi Asintel Kasal dalam melakukan kegiatan siber diantaranya deteksi anomali dan ancaman dalam lingkup sistem dan jaringan TNI AL, melakukan patroli siber terhadap akun-akun media sosial prajurit dan keluarga TNI AL serta pejabat di tingkat Mabesal dan Mabes TNI.

Adapun jumlah personel Labpamsisjar dari awal didirikannya hinga saat tahun 2023 DSP Labpamsisjarb sudah banyak mengalami perubahan dengan jumlah personel sebanyak 69 personel dengan rincian sebagai berikut:

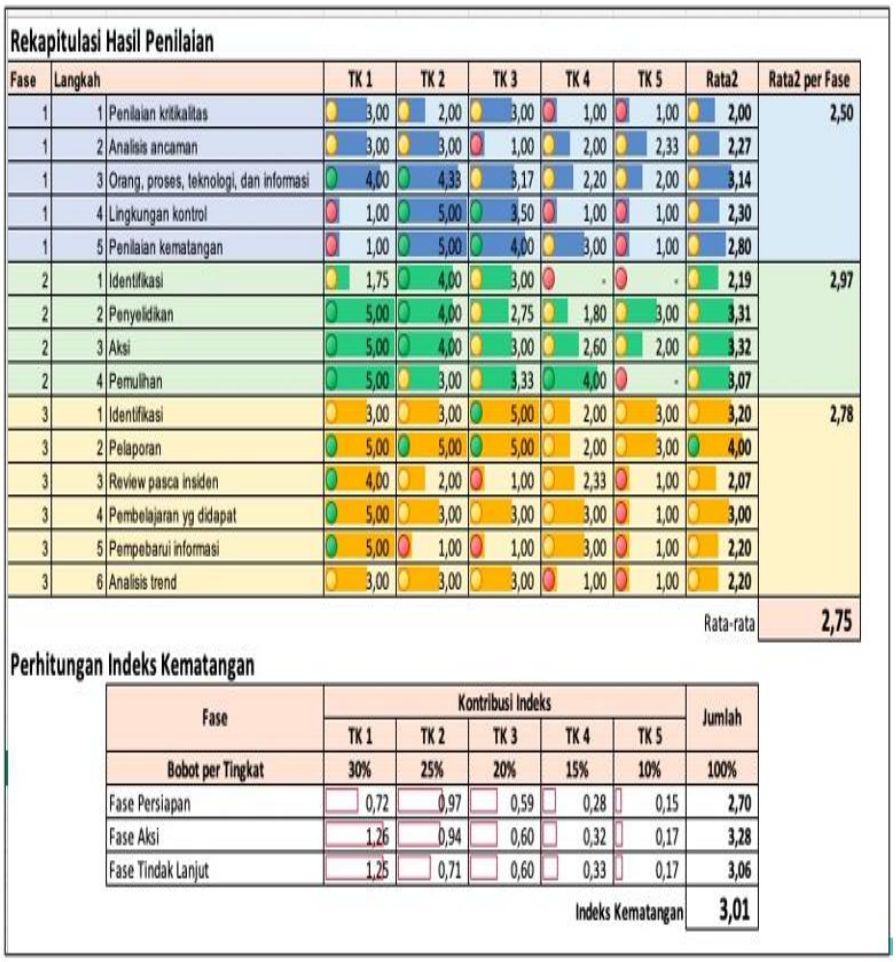
1) Perwira : 28 personel;
2) Bintara : 15 personel;
3) Tamtama : 2 personel; dan
4) PNS : 13 personel.

Berdasarkan hasil evaluasi akhir perhitungan beban kerja Labpamsisjar melalui aplikasi e-kinerja TNI AL diperoleh data perhitungan indeks beban kerja Labpamsisjar diperoleh hasil akhir dengan nilai 144,59%, dengan perincian sebagai berikut:

1) Unsur Pimpinan 146,99%
2) Unsur Pelayanan 145,66%
3) Unsur Pelaksana yang teridri atas Silabdatin 136,61%, Silabkatjarap 140,83% dan Sianalevsimfor 144,59%.

Hasil evaluasi akhir perhitungan beban kerja tersebut menunjukan bahwa nilai Indeks Beban Kerja (IBK) Labpamsisjar diatas 140%. Nilai IBK tersebut diasumsikan menunjukkan bahwa beban kerja yang diterima oleh personil melebihi kapasitasnya dan dapat berdampak pada kesehatan fisik dan mental personil Labpamsisjar.

Hasil penilaian TMPI Keamanan Siber TNI Angkatan Laut adalah sebesar 3,46 atau berada pada level *established* dalam artian bahwa TNI Angkatan Laut sudah melaksanakan tata kelola dan mekanisme kerja terkait penanganan insiden siber berikut dengan sarana prasarana utama yang dibutuhkan sehingga direkomendasikan untuk melaksanakan peresmian CSIRT di Tahun 2022.



Rekapitulasi Hasil Penilaian

Fase	Langkah		TK 1	TK 2	TK 3	TK 4	TK 5	Rata2	Rata2 per Fase
1	1	Penilaian kritikalitas	3,00	2,00	3,00	1,00	1,00	2,00	2,50
1	2	Analisis ancaman	3,00	3,00	1,00	2,00	2,33	2,27	
1	3	Orang, proses, teknologi, dan informasi	4,00	4,33	3,17	2,20	2,00	3,14	
1	4	Lingkungan kontrol	1,00	5,00	3,50	1,00	1,00	2,30	
1	5	Penilaian kematangan	1,00	5,00	4,00	3,00	1,00	2,80	
2	1	Identifikasi	1,75	4,00	3,00	-	-	2,19	2,97
2	2	Penyelidikan	5,00	4,00	2,75	1,80	3,00	3,31	
2	3	Aksi	5,00	4,00	3,00	2,60	2,00	3,32	
2	4	Pemulihan	5,00	3,00	3,33	4,00	-	3,07	
3	1	Identifikasi	3,00	3,00	5,00	2,00	3,00	3,20	2,78
3	2	Pelaporan	5,00	5,00	5,00	2,00	3,00	4,00	
3	3	Review pasca insiden	4,00	2,00	1,00	2,33	1,00	2,07	
3	4	Pembelajaran yg didapat	5,00	3,00	3,00	3,00	1,00	3,00	
3	5	Pempebarui informasi	5,00	1,00	1,00	3,00	1,00	2,20	
3	6	Analisis trend	3,00	3,00	3,00	1,00	1,00	2,20	
							Rata-rata		2,75

Perhitungan Indeks Kematangan

Fase	Kontribusi Indeks					Jumlah
	TK 1	TK 2	TK 3	TK 4	TK 5	
Bobot per Tingkat	30%	25%	20%	15%	10%	100%
Fase Persiapan	0,72	0,97	0,59	0,28	0,15	2,70
Fase Aksi	1,26	0,94	0,60	0,32	0,17	3,28
Fase Tindak Lanjut	1,25	0,71	0,60	0,33	0,17	3,06
					Indeks Kematangan	3,01

Tabel Hasil Penilaian TMPI Keamanan Siber Labpamsisjar dari BSSN

Beberapa permasalahan pada Labpamsisjar saat ini akan dapat menimbulkan beberapa implikasi yang tidak optimal pada kemampuan Labpamsisjar dalam mengamankan infrastriktur informasi vital TNI Angkatan Laut diantaranya:

a. Belum optimalnya pemenuhan sumber daya manusia sesuai dengan kebutuhan DSP dan kompetensi siber personil Labpamsisjar maka akan berdampak pada rendahnya kemampuan Labpamsisjar dalam mengamankan infrastruktur informasi vital TNI Angkatan Laut sehingga mengakibatkan tidak terwujudnya keamanan siber di lingkungan TNI Angkatan Laut.

b. Belum optimalnya Organisasi terkait dengan penetapan kebijakan/ regulasi Validasi Organisasi Labpamsisjar dan penerapan SOP di lingkungan kerja Labpamsisjar maka akan berdampak pada rendahnya kemampuan Labpamsisjar dalam mengamankan infrastruktur informasi vital TNI Angkatan Laut sehingga mengakibatkan tidak terwujudnya keamanan siber di lingkungan TNI Angkatan Laut.

c. Belum optimalnya pengadaan sarana dan prasarana teknologi keamanan siber Labpamsisjar maka akan berdampak pada rendahnya kemampuan Labpamsisjar dalam mengamankan infrastruktur informasi vital TNI Angkatan Laut sehingga mengakibatkan

tidak terwujudnya keamanan siber di lingkungan TNI Angkatan Laut.

d. Belum terwujudnya keamanan siber di lingkungan TNI Angkatan Laut sebagai akibat dari masih rendahnya kemampuan Labpamsisjar dalam mengamankan infrastruktur informasi vital.

Beberapa hal yang menjadi faktor dan mempengaruhi kemampuan Labpamsisjar saat ini diantarnya:

- **Faktor Eksternal**

Ancaman Keamanan Siber.

Perkembangan teknologi telah meningkatkan ancaman terhadap keamanan siber sehingga menjadi kewajiban bagi Labpamsisjar untuk senantiasa meningkatkan kewaspadaan terhadap ancaman siber yang berasal dari negara lain, kelompok peretas (hacker) atau kelompok teroris/ separatis. Ancaman tersebut dapat memiliki dampak yang serius terhadap keamanan dan stabilitas nasional karena berpotensi menjadi serangan yang menargetkan Infrastruktur Informasi Vital (IIV) yang menjadi aset nasional. Ancaman yang paling besar kemungkinan bisa terjadi bilamana informasi-informasi yang bernilai strategis dan berklasifikasi sangat rahasia jatuh ke tangan pihak yang tidak bertanggungjawab akan berpengaruh terhadap kedaulatan negara dan keutuhan wilayah NKRI. TNI menyadari semakin besarnya tantangan dalam menjaga kedaulatan bangsa dan negara termasuk yang memasuki kedaulatan di dunia maya. Melihat realita, fakta- fakta dan mempertimbangkan segala hakekat ancaman yang bakal dihadapi tersebut maka diperlukan kemampuan optimal Labpamsisjar dalam mengatasi ancaman tersebut. Adapun beberapa ancaman yang dimaksud diantaranya:

1) Ancaman siber global, yaitu ancaman siber yang berasal dari negara lain, melibatkan serangan siber yang dilakukan oleh aktor negara (*state actor*) baik oleh pemerintah, badan intelijen,dan kelompok peretas tertentu. Tujuan serangan ini bermacam-macam mulai dari pencurian data sensitif, sabotase infrastruktur kritis, spionase industri, mengganggu layanan (*disruption of service*), atau merusak sistem dan jaringan komputer dengan menggunakan teknik-teknik berbahaya seperti *malware*, *ransomware*, *phishing*, *denial of service*, dan lain-lain. Kejahatan siber tersebut bahkan digunakan untuk mencuri informasi rahasia, mempengaruhi opini publik, atau merusak infrastruktur komunikasi dan keuangan suatu negara.

2) Kelompok peretas. Kelompok peretas, atau *hacker*, adalah individu atau kelompok yang memiliki keahlian teknis untuk meretas sistem komputer dan jaringan dengan tujuan mencuri data, merusak atau mengubah informasi, atau menciptakan kerusakan lainnya. Motivasi mereka dapat bervariasi, termasuk pencurian identitas, pencurian data pribadi atau keuangan, atau privasi.

3) Kelompok teroris/ separatis. Kelompok teroris atau separatis dapat menggunakan serangan siber sebagai alat

untuk mencapai tujuan mereka. Serangan siber oleh kelompok-kelompok ini mungkin mencakup penyebaran propaganda, pencurian dana melalui serangan keuangan digital, penyerangan situs web atau jaringan pemerintah, atau mengekspos kerentanan keamanan.

- **Faktor Internal**

a. Sumber Daya Manusia.

Labpamsisjar Dispamsanal dalam pelaksanaan tugasnya didukung oleh kekuatan personil yang memiliki kemampuan terlatih dan berkualifikasi dibidang keamanan siber. Menyikapi perkembangan teknologi yang kian pesat tentunya kemampuan siber personil Labpamsisjar harus tetap terjaga dan bila perlu ditingkatkan. Pengembangan kompetensi dan kualitas personel Labpamsisjar ditempuh melalui pelatihan, pendidikan, dan program pengembangan kemampuan sertifikasi yang bertujuan untuk meningkatkan keterampilan, pengetahuan, dan profesionalisme personel. Program ini akan menghasilkan personel yang lebih kompeten, adaptif, dan siap menghadapi tugas-tugas yang kompleks.

b. Budaya Keamanan Siber.

Menumbuhkembangkan budaya keamanan siber dikalangan personel TNI AL perlu dilakukan dalam rangka memberi pengetahuan dan kesadaran akan pentingnya keamanan siber. Dalam prakteknya personil Labpamsisjar dalam melakukan deteksi, monitoring dan patroli siber sering menemukan banyaknya ancaman pada aplikasi sistem informasi dan jaringan komputer satuan kerja TNI AL. Dari hasil analisa intelijen siber Labpamsisjar ditemukan bahwa salah satu ancaman siber itu muncul dari lingkungan satuan kerja (satker) di lingkungan TNI AL. Umumnya *malware, virus, ransomware* dan *spyware* akan menginfeksi perangkat komputer atau labtop di satker melalui pengunaan *flashdisk*, *smartphone*, *memory card* dan *device* lainnya sehingga perlu dibuat aturan atau protokol yang jelas untuk dipatuhi.

c. Infrastruktur dan Teknologi.

Labpamsisjar sebagai laboratorium siber membutuhkan infrastruktur dan teknologi yang memadai untuk melakukan tugas pengamanan IIV TNI AL yang meliputi perangkat keras (hardware) dan perangkat lunak (software) yang diperlukan untuk melaksanakan kegiatan keamanan siber diantaranya pemantauan jaringan, simulasi serangan, analisis forensik dan tugas-tugas keamanan siber lainnya. Ketersediaan perangat keamanan siber yang modern dan up-to-date diantaranya penggunaan firewall, enkripsi dan sistem deteksi intrusi akan meningkatkan kemampuan laboratorium sehingga akan mendukung terwujudnya keamanan siber TNI AL.

d. Standar Operasional Prosedur.

Penerapan metodologi dan proses yang efektif dalam pelaksanaan tugas-tugas juga turut mempengaruhi kemampuan siber Labpamsisjar. Penggunaan kerangka kerja (*framework*) terstandarisasi, Standar Operasional Prosedur (SOP), dan metode investigasi yang sistematis akan membantu meningkatkan efisiensi dan akurasi pekerjaan personil Labpamsisjar dalam pelaksanaan

tugas mengamankan IIV dalam rangka mewujudkan keamanan siber TNI AL.

e. Manajemen Risiko.

Labpamsisjar dalam melaksanakan tugas keamanan siber, perlu menerapkan manajemen risiko melalui identifikasi risiko secara teratur, evaluasi kerentanan, dan pengelolaan risiko untuk mengurangi potensi serangan dan dampaknya. Manajemen risiko bertujuan mengurangi potensi dampak ancaman atau serangan siber seperti *malware*, *DDoS* dan kebocoran data, kerentanan dalam sistem, serta dampak yang mungkin terjadi jika risiko terwujud (seperti kerugian keuangan, reputasi yang rusak, atau ketidaktersediaan data pada sistem).

f. Kerjasama Internal.

Dalam pelaksanaan tugasnya Labpamsisjar Dispamsanal memiliki 3 (tiga) Sie Laboratorium (Silab) yang terdiri atas Laboratorium Data dan Informasi (Silab datin), Laboratorium Perangkat, Jaringan dan Aplikasi (Silab Katjarap), dan Laboratorium Analisa, Evaluasi, Simulasi dan Forensik (Silab Analevsimfor). Ketiga Silab ini saling bersinergi dalam mengamankan IIV TNI AL.

4. KESIMPULAN.

a. Dalam rangka mengamankan infrastruktur informasi vital TNI Angkatan Laut dibutuhkan sumberdaya manusia yang memadai baik dari segi kualitas maupun kuantitas. Pemenuhan kebutuhan sumber daya manusia secara kuantitas atau jumlah dilaksanakan dengan penambahan jumlah personel melalui perekrutan secara formal maupun melalui penugasan dari satuan kerja lain di lingkungan TNI Angkatan Laut untuk memenuhi kebutuhan personil sesuai DSP dan struktur organisasi Labpamsisjar, serta melaksanakan peningkatan kompetensi personil melalui pendidikan, pelatihan dan sertifikasi bidang keamanan siber.

b. Kebijakan/ regulasi terkait validasi organisasi Lapamsisjar menjadi Satuan Siber TNI Angkatan Laut dan penerapan SOP di lingkungan Labpamsisjar juga diperlukan guna mendukung Labpamsisjar dalam mengamankan Infrastruktur Informasi Vital. Hal ini sejalan dengan kebijakan pemerintah yang didasarkan pada Peraturan Presiden Nomor 43 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Risiko Siber serta Permenhan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

c. Pengamanan Infrastruktur Informasi Vital (IIV) TNI AL dalam rangka mewujudkan keamanan siber dapat dilakukan dengan dukungan kemampuan sarana dan prasarana yang modern dan *update* sesuai dengan perkembangan teknologi keamanan siber sehingga perangkat teknologi (perangkat keras dan perangkat lunak) yang digunakan dapat mengatasi segala bentuk ancaman dan potensi serangan siber yang semakin kompleks. Disisi lain perangkat teknologi yang digunakan tidak dapat berdiri sendiri tanpa adanya pengawak baik sebagai operator maupun sebagai analis ancaman yang keduanya dituntut mampu bekerja di dalam SOP yang sudah dibuat untuk mengurangi risiko yang akan timbul.

5. REFERENSI.

A. Buku dan Barang Cetakan.

Balai Pustaka. (1997). Kamus Besar Bahasa Indonesia, edisi kedua

Hasibuan H. Malayu. (1996). Organisasi dan Motivasi, Dasar Peningkatan Produktivitas, Jakarta.

HC Chotimah. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian …", Jurnal Politica Dinamika Masalah Politik Dalam … Jurnal.dpr.go.id.Malayu, S.P.,

Hasibuan, H, Drs. (2009). Manajemen Sumber Daya Manusia Cetakan 12, PT. Bumi Aksara, Jakarta.

Matutina. (2001). Manajemen Sumber daya Manusia Cetakan Kedua, Gramedia Widia Sarana Indonesia, Jakarta.

Nawawi, Hadari. (2005). Perencanaan SDM Untuk Organisasi Profit Yang Kompetitif, Penerbit Gajah Mada University Press, Yogyakarta.

Sulistiani. A.T. & Rosidah (2003). Manajemen Sumber Daya Manusia, Jakarta.

S Hidayati and RAG Gultom. (2020). Analisis Kebutuhan Senjata Siber Dalam Meningkatan Pertahanan Indonesia Di Era Peperangan Siber", *Teknologi Persenjataan*. Jurnal Prodi.idu.ac.id.

Tjiptono, Fandy. (2004). Manajemen Jasa Edisi Kedua, Andi Offset, Yogyakarta.

W. Richard Scott. (2004). Institutional Theory: Contributing to a Theoretical Research Program", dalam Ken G. Smith and Michael A. Hitt (eds), Great Minds in Management: The Process of Theory Development. Oxford University Press, Oxford.

Wirawan. (2008). Evaluasi Kinerja Sumber Daya Manusia, Salemba Empat, Jakarta.

Wibowo. (2007). Manajemen kinerja, PT. Raja Grafindo Persada.

Wursanto.LG. (2003). Dasar–Dasar Ilmu Organisasi, PT.ANDI, Yogyakarta.

B. Terbitan Berkala.

BSSN. (2018). Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019.

Laporan Tahunan. Tahun 2020, Honeynet-BSSN.

Laporan Tahunan. Tahun 2021, Monitoring Keamanan Siber. BSSN.

Lanskap Keamanan Siber Indonesia. Tahun 2022, BSSN.

Laporan Tahunan. Tahun 2022, Labpamsisjar-Dispamsanal. TNI AL.

C. Publikasi Elektronik.

http://www.artikelsiana.com/2015/10/manajemen-sumber-daya-manusia.html

https://www.teknovidia.com/serangan-siber-cyber-attack/. Diakses tanggal 18 Juli 2023

https://peraturan.bpk.go.id/Home/Details/174292/peraturan-bssn-no-4-tahun-2019

https://nasional.sindonews.com/read/1248299/14/bentuk-satuan-siber-tni-siap-hadapi-serangan-di-duniamaya-1507966324

D. Peraturan-peraturan.

Undang-Undang Republik Indonesia nomor 3 tahun 2002 tentang Pertahanan Negara.

Undang-Undang Republik Indonesia nomor 34 tahun 2004 tentang Tentara Nasional Indonesia

Undang-Undang Nomor 18 Tahun 2008 tentang Keterbukaan Informasi Publik.

Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.

Peraturan Presiden Nomor 66 Tahun 2022 tentang Organisasi Tentara Nasional.

Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital.

Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 3 Tahun 2021 tentang Peraturan Pelaksanaan Undang-Undang Nomor 23 tahun 2019 tentang Pemberdayaan Sumber Daya Nasional untuk Pertahanan Negara.

Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pertahanan Siber;

Keputusan Panglima TNI Nomor Kep/555/VI/2018 tanggal 6 Juni 2018 tentang Doktrin Tentara Nasional Indonesia Tri Dharma Eka Karma sebagaimana Perubahan I Keputusan Panglima TNI Nomor Kep/555.a/VI/2018 tanggal 1 Juli 2019 tentang Doktrin Tentara Nasional Indonesia Tri Dharma Eka Karma.

Keputusan Panglima TNI Nomor Kep/1001/XII/2020 tanggal 16 Desember 2020 tentang Petunjuk Penyelenggaraan Operasi Siber Tentara Nasional Indonesia.

Peraturan Panglima TNI Nomor 3 Tahun 2018 tentang Organisasi dan Tugas Satuan Marinir Komando Armada, Satuan Udara Komando Armada, Laboratorium Pengamanan Sistem dan Jaringan serta Detasemen Markas Komando Utama TNI Angkatan Laut.

Keputusan Panglima TNI Nomor Kep/1355/XII/2018 tanggal 18 Desember 2018 tentang Doktrin Siber Tentara Nasional Indonesia.

Keputusan Kepala Staf Angkatan Laut Nomor Kep / 2551 / Vlll / 2020 Tentang Daftar Susunan Personel Pada Organisasi Markas Besar TNI Angkatan Laut Bagian Ketiga.

Peraturan Kasal Nomor 12 Tahun 2018 tentang Pembentukan Laboratorium Pengamanan Sistem dan Jaringan.

Keputusan Kasal Nomor 1457/VI/2018 tentang Daftar Susunan Personil pada Organisasi Laboratorium Pengamanan Sistem dan Jaringan.

Peraturan Kasal Nomor 24 Tahun 2018 tentang Organisasi dan Prosedur Laboratorium Pengamanan Sistem dan Jaringan.