KONSEP PEMBANGUNAN TEKNOLOGI PERTAHANAN *CYBER SECURITY* BERBASIS *SIX WARE FRAMEWORK* DI MARKAS KOMANDO PANGKALAN TENTARA NASIONAL INDONESIA ANGKATAN LAUT PALU

DEVELOPMENT CONCEPT OF CYBER SECURITY DEFENSE TECHNOLOGY BASED ON SIX WARE FRAMEWORK AT THE HEAD OF THE INDONESIAN NATIONAL ARMY BASE OF THE PALU NAVY COMMAND

Nyoman Darmawan[1], Aris Poniman[2], Rudy A.G Gultom[3]

[1,2,3]PROGRAM STUDI TEKNOLOGI PENGINDERAAN, UNIVERSITAS PERTAHANAN

(komandar1976@gmail.com, arispk2007@gmail.com, rudygultom67@gmail.com)

Abstrak – Teknologi informasi dan komputer di Mako Lanal Palu selalu berkaitan dengan *cyberspace*. Instansi Militer adalah bagian integral yang paling utama dari kemampuan pertahanan suatu negara sehingga kemungkinan mendapatkan serangan siber untuk mendisrupsi proses penyelengaraan pertahanan atau mencuri data rahasia oleh aktor *state* maupun *non-state* adalah sangat tinggi. Tujuan penelitian ini untuk menganalisis dan mendeskripsikan kondisi sistem pertahanan siber di Mako Lanal Palu saat ini berdasarkan SWCS dan untuk merumuskan konsep pembangunan teknologi pertahanan sebagai pendukung *cyber security* di Mako Lanal Palu berdasarkan konsep SWCS. Penelitian ini menyajikan pendekatan "SWCSF" untuk memahami implementasinya sesuai karakteristik instansi pertahanan militer di Lanal Palu. Penelitian ini menggunakan metode campuran: survei dan pendekatan statistik inferensial. Pengumpulan data di lokus dengan kuesioner terhadap 21 responden dan wawancara kepada informan yang terkait di Lanal Palu. Hasil penelitian ini menunjukkan bahwa "SWCSF" sangat cocok diterapkan di instansi pertahanan militer. berdasarkan analisis kualitatif Lanal Palu belum mampu menangani adanya ancaman/serangan siber karena belum ada bidang khusus (peta jabatan) dalam struktur organisasi Lanal Palu dan belum adanya SDM yang secara khusus berkualifikasi IT dan keamanan siber yang bertanggung jawab terkait keamanan siber dan IT serta belum ada rencana untuk program kerja dan anggaran sedangkan analisis kuantitatif kemampuan teknologi pertahanan siber berbasis SWCSF di Mako Lanal Palu dalam menghadapi ancaman siber dalam kategori baik. bahwa SWCSF memiliki keunggulan berupa kemudahan implementasi dalam mengukur kesiapan suatu organisasi terhadap ancaman/serangan siber.

Kata Kunci: ancaman/serangan siber, metode campuran, statistik inferensial, *Six Ware Cyber Security Framework* (SWCSF), teknologi pertahanan siber.

Abstract – *Information technology and computers at the head* of The Indonesian National Army Base of The Palu Navy Command *are always related to cyberspace. Military agencies are the most important integral part of a country's defense capability, so the possibility of getting cyber attacks to disrupt the defense administration process or steal confidential data by state and non-state actors is very high. The purpose of this study is to analyze and describe the current state of the cyber defense system at the head* of The Indonesian National Army Base of The Palu Navy Command *based on SWCS and to formulate the concept of developing defense technology as a support for cyber security at the head* of The Indonesian National Army Base of The Palu Navy Command *based on the SWCS concept. This study presents a "SWCSF" approach to understand its implementation according to the characteristics of the military defense agency at the head* of The Indonesian National Army Base of

The Palu Navy Command. *This study uses a mixed method: survey and inferential statistical approaches. Data collection at the locus with a questionnaire to 21 respondents and interviews with relevant informants in Indonesian National Navy (TNI) Base Command Headquarters at Palu. The results of this study indicate that "SWCSF" is very suitable to be applied in military defense agencies. based on qualitative analysis, The head* of The Indonesian National Army Base of The Palu Navy Command *has not been able to handle cyber threats / attacks because there is no special field (job map) at the head* of The Indonesian National Army Base of The Palu Navy Command *organizational structure and there is no HR specifically qualified for IT and cybersecurity who is responsible for cyber security and IT and does not exist plans for work programs and budgets while the quantitative analysis of the ability of SWCSF-based cyber defense technology at the head* of The Indonesian National Army Base of The Palu Navy Command *in facing cyber threats is in a good category. that SWCSF has the advantage of ease of implementation in measuring the readiness of an organization against cyber threats / attacks.*

***Keywords**: cyber defense technology, cyber threats / attacks, mixed methods, inferential statistics, Six Ware Cyber Security Framework (SWCSF)*

Pendahuluan

Salah satu temuan yang memberikan pengaruh paling besar dalam masyarakat informasi adalah ditemukannya internet. Hadirnya internet sebagai bentuk teknologi baru menyebabkan manusia tidak mampu terlepas dari arus komunikasi dan informasi. Internet telah menyebabkan terjadinya satu lompatan besar dalam kehidupan. Sama halnya dengan teknologi lainnya, internet tidak bebas nilai. Teknologi akan menjadi efektif jika kita memberi perhatian pada kegunaan dari teknologi yang disesuaikan dengan nilai-nilai sosial maupun pribadi serta adanya peraturan pemerintah yang melindungi masyarakat dari dampak negatif yang ditimbulkannya (Ardiyanti, 2014). Dampak negatif yang dimaksud tersebut adalah munculnya cybercrime. *Cybercrime* merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet (Ketaren, 2016). Hal tersebut dibuktikan dengan data yang dirilis oleh Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara dimana terdapat sebanyak 88.414.296 cyber attack yang telah terjadi di Indonesia sejak 1 Januari - 12 April 2020 (Dewi, 2020). Pada bulan Januari terpantau 25.224.811 serangan dan kemudian pada bulan Februari terekam 29.188.645 serangan lalu kemudian pada bulan Maret terjadi 26.423.989 serangan dan sampai dengan 12 April 2020 telah tercatat 7.576.851 serangan. Puncak jumlah serangan terjadi pada tanggal 12 Maret 2020 yang mencapai 3.344.470 serangan dan setelah itu jumlah serangan

mengalami penurunan yang cukup signifikan saat diberlakukannya kebijakan *Work From Home* (WFH) di berbagai tempat (BSSN, 2020). Tentunya hal ini akan menimbulkan kekacauan dan kerugian dari berbagai kalangan. Gambaran tersebut merupakan contoh dampak yang diakibatkan oleh *cyber attack* yang bisa lebih menghancurkan dan mengacaukan dibanding serangan fisik. Banyak definisi tentang serangan siber, namun dalam Permenhan nomor 82 tahun 2014 tentang Pedoman Pertahanan Siber dijelaskan bahwa cyber attack adalah segala bentuk perbuatan, perkataan, pemikiran baik yang dilakukan dengan sengaja maupun tidak sengaja oleh pihak mana pun, dengan motif dan tujuan apapun, yang dilakukan di lokasi manapun, yang disasarkan pada sistem elektronik atau muatannya maupun peralatan yang sangat bergantung pada teknologi dan jaringan dalam skala apa pun, terhadap obyek vital maupun non-vital dalam lingkup militer dan non-militer, yang mengancam kedaulatan negara, keutuhan wilayah dan keselamatan bangsa (Sataloff et al., 2011). Secara lebih spesifik organ pertahanan Indonesia juga pernah mendapatkan serangan tersebut ketika salah satu situs resmi unit kerja Kementerian Pertahanan Republik Indonesia dibobol oleh hacker, yakni website milik Direktorat Jenderal Potensi Pertahanan yang mengalami perubahan laman yang disebut defacing. Situs Ditjen Pothan tersebut dibobol oleh CVT pada 2018 (D. A. Putra et al., 2020). Selain website resmi milik Kementerian Pertahanan, website resmi milik Kementerian Dalam Negeri juga pernah diretas oleh hacker pada September 2019, sebagai bentuk aksi protes terhadap diterbitkannya revisi Undang-Undang Komisi Pemberantasan Korupsi. Bahkan yang terbaru adalah, peretasan website DPR RI dimana halaman muka situs web DPR yang tulisannya diubah menjadi «Dewan Pengkhianat Rakyat» pada tanggal 7 Oktober 2020, sebagai buntut kekecewaan masyarakat atas di sah kannya RUU Omnimbus Law (maharani, 2020). Melihat betapa mengerikannya ancaman *cyber attack* tersebut, maka sudah semestinya pemerintah Indonesia membangun *cyber security* dengan di dukung teknologi pertahanan yang mumpuni, mengingat hakekat ancaman sekarang ini yang tidak hanya ancaman yang bersifat militer semata melainkan

ancaman yang bersifat nirmiliter, salah satunya berupa ancaman serangan cyber (Sa'diyah & Vinata, 2016). Bahkan di negara maju angkatan pertahanan cyber adalah matra ke empat setelah Matra Darat, Laut dan Udara (Riza, 2017). Saat ini di Pangkalan TNI AL Palu masih didukung sebanyak 17 perangkat komputer yang digunakan sebagai penunjang kerja mereka. Selain itu, untuk mendukung operasionalisasi kerja jarak jauh, di Pangkalan TNI AL Palu juga didukung oleh jaringan internet yang bekerja sama dengan pihak PT. Telkom. Selain itu, baru-baru ini Pangkalan TNI AL Palu juga di berikan 2 unit perangkat komputer yang secara khusus hanya digunakan oleh bagian yang mengurus keuangan. Adanya fasilitas tersebut, rupanya bak pisau bermata dua. Selain juga memberikan manfaat serta dukungan bagi kinerja anggota yang bertugas di Pangkalan TNI AL Palu, tetapi juga memberikan celah atau kelemahan-kelemahan yang menjadi hambatan atau kesenjangan. Hambatan atau kesenjangan tersebut diantaranya adalah belum adanya Local Area Network yang menghubungkan masing-masing perangkat komputer yang ada di Pangkalan TNI AL Palu; belum adanya bagian khusus yang menangani *maintenance computer*, sehingga masih menggunakan pihak kedua yang tentu saja bisa menjadi potensi ancaman baru; hampir keseluruhan software yang digunakan tidak original; dan Keahlian pengawak/operator komputer masih terbatas dan minim pengetahuan tentang *cyber*. Adanya permasalahan, maka perlu untuk dilakukan pembangunan teknologi pertahanan di Pangkalan TNI AL Palu yang terdampak arus perkembangan teknologi yang sangat cepat, dimana pengembangan teknologi tersebut dapat dibangun berdasarkan konsep Six-Ware Cyber Security. Hal tersebut didukung dengan hasil penelitian yang ditemukan oleh Gultom, Farid, Lestari, Lahallo, & Akbar (R A G Gultom et al., 2020) yang menyatakan bahwa dengan menerapkan konsep *Six-Ware Cyber Security* sebuah organisasi akan lebih memiliki kesiapan dalam menghadapi timbulnya ancaman cyber. Penelitian yang dilakukan oleh Gultom et al diatas, merupakan tindak lanjut dari penelitian-penelitian yang dilakukan sebelumnya, dimana yang pertama

yakni dilakukan pada tahun 2016 yang membahas terkait peningkatan lingkungan keamanan jaringan dengan memberdayakan pemodelan dan strategi simulasi. Menurut Gultom & Alrianto (Rudy Agus Gemilang Gultom & Alrianto, 2016) temuan dalam penelitiannya menjelaskan bahwa Penerapan strategi pertahanan yang tepat dapat mengamankan Local Area Network suatu organisasi dari berbagai ancaman, serangan dan kerentanan pada tingkat konkrit dan abstrak. Bahwa Kedepannya, konsep SWNSF perlu diimplementasikan dan dikembangkan secara lebih mendalam penelitian lebih lanjut tentang area tertentu, misalnya, menentukan keamanan yang lebih teknis dan khusus variabel kerangka kerja, sub-variabel, indikator, referensi informasi, skor indeks keamanan dan lain-lain (Gemilang Gultom et al., 2018). Selanjutnnya pemanfaatan teknologi dan pertahanan *cyber* dapat meningkatkan sistem pertahanan organisasi, bahwa ancaman Siber merupakan ancaman nyata yang saat ini dan menjadi pokok perhatian dari para stakeholder tingkat nasional maupun di tingkat TNI. Dalam menghadapi ancaman siber yang ada khususnya yang mengancam kedaulatan negara dan keutuhan wilayah NKRI serta mengancam keselamatan seluruh bangsa dan negara, maka TNI membentuk Satuan Siber TNI sebagai leading sector dalam membangun pertahanan siber dalam rangka mendukung sistem pertahanan militer serta dibutuhkan strategi yang tepat untuk mewujudkannya (R. D. Putra & Deni, 2018)

Rumusan masalah dari penelitian ini yaitu:

a. Bagaimana kondisi sistem pertahanan siber di Mako Lanal Palu saat ini berdasarkan *Sixware Framework*?
b. Bagaimana Membangun Teknologi Pertahanan sebagai pendukung cyber security di Pangkalan TNI AL Palu berdasarkan konsep *Six-Ware Cyber Security?*

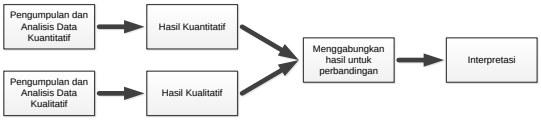
Tujuan yang ingin dicapai dalam penelitian ini adalah:

a. Untuk menganalisis dan mendeskripsikan kondisi sistem pertahanan siber di Mako Lanal Palu saat ini berdasarkan *Sixware Framework*.
b. Untuk merumuskan konsep pembangunan Teknologi Pertahanan sebagai pendukung *cyber security* di

Pangkalan TNI AL Palu berdasarkan konsep *Six-Ware Cyber Security*.

Metode Penelitian

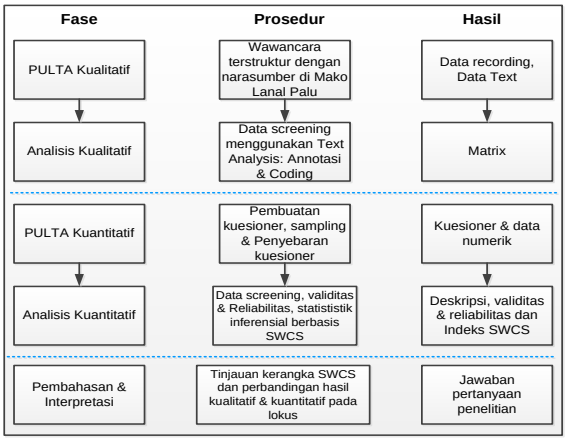
Penelitian ini dilakukan dengan menggunakan metode mixed methods yaitu suatu langkah penelitian dengan menggabungkan dua bentuk pendekatan penelitian yang mengkombinasikan antara penelitian kuantitatif dan kualitatif (sugiyono, 2017). Mixed methods dilakukan untuk meminimalisir beberapa kelemahan yang akan muncul apabila peneliti hanya menggunakan salah satu metode diantara kuantitatif dan kualitatif. Sedangkan dalam penelitian ini, disain dasar yang akan dipilih adalah disain konvergen (Creswell, J. W. & Clark, 2018). Disain konvergen pengumpulan data kuantitatif dan kualitatif dilakukan secara paralel, menganalisis masing-masing data, membandingkan hasilnya, dan menjelaskan kesamaan dan ketidaksesuaian hasilnya.



Gambar 1. Rancangan Konvergen
Sumber: Cresswell & Clark, 2018

Desain Penelitian

Data kualitatif dihimpun melalui wawancara dengan pakar di lokus dan data kuantitatif diperoleh melalui kuesioner. Penelitian kuantitatif melalui penyebaran kuesioner dilakukan untuk mengetahui kondisi teknologi *cyber defense* yang dimiliki oleh Lanal Palu terhadap ancaman atau serangan siber.



Gambar 2. Disain Penelitian
Sumber: diolah oleh peneliti, 2020

Populasi dan Sampel

Populasi dalam penelitian ini adalah seluruh personel TNI AL yang bertugas di Mako Lanal Palu yang pernah atau sedang memanfaatkan teknologi informasi baik yang berhubungan dengan Alutsista maupun dengan sistem informasi manajemen yang ada di kantor dengan jumlah sebanyak 130 orang.

Ukuran sampel dihitung berdasarkan rumus slovin:

$$n = \frac{N}{1+N(e)^2}$$

Keterangan:

n = Ukuran sampel/jumlah responden

N = Ukuran populasi

e = Presentase kelonggaran ketelitian kesalahan pengambilan sampel yang masih bisa ditolerir

Dengan ketentuan sebagai berikut:

Nilai e = 0,1 (10%) populasi jumlah besar

Nilai e = 0,2 (20%) populasi jumlah kecil

Jadi rentang sampel diambil dari teknik Slovin adalah antara 10-20% dari populasi. Oleh karena jumlah populasi dari lokus tergolong kecil (< 200), maka digunakan tingkat kesalahan 20%. Berdasarkan rumus slovin diatas, maka jumlah sampel yang digunakan dalam adalah sebanyak 21 orang

Hasil dan Pembahasan

Hasil Analisis Data Kualitatif

Dari hasil wawancara terhadap para informan dengan menggunakan media wawancara (*interview guide*), maka diperoleh fakta-fakta di lapangan:

Tabel 1. Hasil Analisis Data Kualitatif

No	Nara sumber	Coding Pengaruh	Deskripsi Coding	Interpretasi
1	Muran to	Positif	Tidak siap	Lanal Palu belum melengkapi Six-Ware untuk mencapai tugas dan fungsinya
2	Astri Y	Positif	Tidak siap	Six-Ware di Lanal Palu belum dapat di laksanakan karena belum ada dalam struktur organisasi (peta jabatan)
3	Yusuf W	Positif	Tidak siap	Lanal Palu belum melengkapi Six-Ware untuk mencapai tugas dan fungsinya

Sumber: Diolah oleh peneliti, 2020

Hasil Analisis Data Kuantitatif

Deskripsi Statistik

hasil perhitungan statistik deskriptif (Sujarweni, 2020) untuk seluruh variabeL Six-Ware (*Brainware*, *Hardware*, *Software, Infrastructureware*, *Firmware*, dan *Budgetware*)

Tabel 2. Deskripsi Data

	N	Range	Min	Max	Sum	Mean	Std Deviation

BW	21	13	41	54	962	45.81	4.285
HW	21	7	18	25	450	21.43	2.181
SW	21	5	20	25	453	21.57	1.989
ISW	21	26	53	79	1385	65.95	7.345
FW	21	8	32	40	707	33.67	2.834
BGW	21	17	38	55	965	45.95	4.141

Sumber: Diolah oleh peneliti, 2020

Validitas dan Reliabilitas

Uji validitas dilakukan dengan menilai korelasi antar variabel dan Uji reliabilitas instrumen dikalkulasi menggunakan Cronbach Alpha.

Brainware

Tabel 3. *Reliability Statistics Brainware*

Cronbach's Alpha	N of Items
.809	**11**

Sumber: Diolah oleh peneliti, 2020

bahwa $R_{Hitung} > R_{Tabel}$ Maka dinyatakan Valid, R_{Tabel} dengan responden 21 orang dengan taraf signifikan 0,05 yaitu 0,369, Jadi R_{Hitung} 0,809 > R_{Tabel} 0,369 dan nilai alpha > 0,60 yaitu 0,809 > 0,60 maka dinyatakan reliabel.

Hardware

Tabel 4. *Reliability Statistics Hardware*

Cronbach's Alpha	N of Items
.907	**5**

Sumber: Diolah oleh peneliti, 2020

bahwa $R_{Hitung} > R_{Tabel}$ Maka dinyatakan Valid, R_{Tabel} dengan responden 21 orang dengan taraf signifikan 0,05 yaitu 0,369, Jadi R_{Hitung} 0,907 > R_{Tebel} 0,369 dan nilai alpha > 0,60 yaitu 0,907 > 0,60 maka dinyatakan reliabel.

Software

Tabel 5. *Reliability Statistics Software*

Cronbach's Alpha	N of Items
.866	**5**

Sumber: Diolah oleh peneliti, 2020

bahwa $R_{Hitung} > R_{Tabel}$ Maka dinyatakan Valid, R_{Tabel} dengan responden 21 orang dengan taraf signifikan 0,05 yaitu 0,369, Jadi R_{Hitung} 0,866 > R_{Tabel} 0,369 dan nilai alpha > 0,60 yaitu 0,866 > 0,60 maka dinyatakan reliabel.

Infrastructureware

Tabel 6. *Reliability Statistics Infrastructureware*

Cronbach's Alpha	N of Items
.926	16

Sumber: Diolah oleh peneliti, 2020

bahwa $R_{Hitung} > R_{Tabel}$ Maka dinyatakan Valid, R_{Tabel} dengan responden 21 orang dengan taraf signifikan 0,05 yaitu 0,369, Jadi R_{Hitung} 0,926 > R_{Tabel} 0,369 dan nilai alpha > 0,60 yaitu 0,926 > 0,60 maka dinyatakan reliabel.

Firmware

Tabel 7. *Reliability Statistics Firmware*

Cronbach's Alpha	*N of Items*
.921	8

Sumber: Diolah oleh peneliti, 2020

bahwa R_{Hitung} > R_{Tabel} Maka dinyatakan Valid, R_{Tabel} dengan responden 21 orang dengan taraf signifikan 0,05 yaitu 0,369, Jadi R_{Hitung} 0,921 > R_{Tabel} 0,369 dan nilai alpha > 0,60 yaitu 0,921 > 0,60 maka dinyatakan reliabel.

Budget ware

Tabel 8. *Reliability Statistics Budget ware*

Cronbach's Alpha	*N of Items*
.902	11

Sumber: Diolah oleh peneliti, 2020

bahwa R_{Hitung} > R_{Tabel} Maka dinyatakan Valid, R_{Tabel} dengan responden 21 orang dengan taraf signifikan 0,05 yaitu 0,369, Jadi R_{Hitung} 0,902 > R_{Tabel} 0,369 dan nilai alpha > 0,60 yaitu 0,902 > 0,60 maka dinyatakan reliabel.

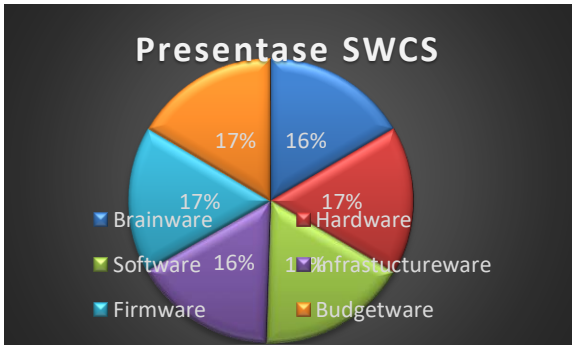
Indeks SWCS

Indeks SWCS terdiri dari Kesiapan: Brainware, Hardware, Software, Infrastructureware, Firmware, dan Budgetware

Tabel 9. Hasil Analisis Kuantitatif Indeks SWCS

Indeks SWCS	**Jumlah**	**Deskripsi**
Brainware	83	Baik
Hardware	85	Baik
Software	86	Baik
Infrastructureware	82	Baik
Firmware	84	Baik
Budgetware	83	Baik
Rata-rata Indeks SWCS	83.83	Baik

Sumber: Diolah oleh peneliti, 2020



Gambar 3. Presentase SWCS
Sumber: diolah oleh peneliti (2020)

Berdasarkan tabel 9 dan gambar 3 diatas, bahwa hasil penilaian secara keseluruhan Indeks SWCS di Mako Lanal Palu adalah baik mulai dari *Software, Hardware*, *Firmware*, *Brainware* dan *Budgetware*, serta *Infrastructureware.*

Interpretasi Hasil Analisis Kualitatif dan Kuantitatif berbasis SWCS

Tabel 10. Penyimpulan Interpretatif

SWCS	Indeks SWCS	Deskripsi Indeks Kuantitatif	Deskripsi Coding Kualitatif	Interpretasi
BW	83	Baik	Tidak Siap	Lanal Palu memiliki teknologi pertahanan siber, namun SDM masih sangat terbatas
HW	85	Baik	Siap	Lanal Palu memiliki hardware dan teknologi pertahanan siber yang cukup
SW	86	Baik	Siap	Lanal Palu memiliki teknologi pertahanan siber dan software, namun belum memiliki rencana pengembangan pertahanan keamanan siber nya
ISW	82	Baik	Tidak Siap	Lanal Palu memiliki teknologi pertahanan siber namun infrastruktur yang belum memadai/belum siap
FW	84	Baik	Tidak Siap	Lanal Palu memiliki teknologi pertahanan siber, akan tetapi belum diatur dalam SOP dan menunggu kebijakan pusat (Kotas)
BgW	83	Baik	Tidak Siap	Lanal Palu memiliki teknologi pertahanan siber, namun belum ada program kerja dan anggaran untuk keamanan sibernya

Sumber: Diolah oleh peneliti, 2020

bahwa secara keseluruhan hasil analisis SWCS di Mako Lanal Palu berupa Indeks SWCS = 83,83 (Baik) dan Coding Kualitatif = "Tidak Siap" dapat diinterpretasikan bahwa Lanal Palu telah memiliki teknologi namun belum memiliki rencana pengembangan teknologi pertahanan keamanan siber dan IT.

Konsep Pembangunan Teknologi Pertahanan *Cyber Security* Berbasis *Six Ware* Mako Lanal Palu

Berdasarkan hasil penelitian yang dilakukan oleh peneliti kepada responden dan informan terkait *Six-Ware Cyber Security Framework*, sistem keamanan siber lanal Palu belum optimal, Lanal Palu belum siap dalam menghadapi ancaman/serangan siber, bahwa hasil penilaian dari keenam

indikator SWCS Pangkalan TNI AL Palu harus banyak melaksanakan pembenahan dan segera merencanakan pembangunan terkait dengan teknologi dan sistem keamanan sibernya.

a. Indikator *Brainware*

1) Agar segera membentuk struktur organisasi (peta jabatan) yang membidangi sistem keamanan siber dan IT Lanal Palu. Dalam struktur organisasi disesuaikan dengan perannya masing-masing apa yang menjadi bidang tugas dan tanggungjawabnya, sebagaimana dalam struktur organisasi disesuaikan dengan jabatan yang sejajar dengan perwira staf Lanal Palu yaitu dijabat oleh seorang perwira menengah berpangkat Mayor.
2) Setelah struktur organisasi (peta jabatan) bidang sistem keamanan siber dan IT Lanal Palu terbentuk dan sudah masuk kedalam DSP (Daftar Susunan Personel) Lanal Palu, segera diikuti dengan penunjukkan pejabat beserta pengawaknya yang membidangi urusan administrasi, teknisi dan operator untuk mengisi jabatan tersebut. Pejabat dan pengawak organisasi yang ditunjuk harus berdasarkan surat telegeram dan surat perintah dari pejabat yang berwenang disesuaikan dengan tugas dan tanggungjawabnya masing-masing, bukan seperti penunjukkan dalam bentuk satgas (satuan tugas), sehingga pejabat dan pengawak bidang keamanan siber dan IT tersebut memiliki payung hukum yang kuat dan bertanggungjawab penuh terkait bidang tugas dan tanggungjawabnya masing-masing, pejabat dan pengawak organisasi bidang keamanan siber dan IT yang ditunjuk dan diberikan tanggungjawab agar disesuaikan juga bidang keahlian dan profesi dengan latar belakang Pendidikan atau disiplin ilmu yang dimiliki, serta diberikan tugas dan tanggungjawabnya masing-masing agar jelas siapa berbuat apa sesuai tugas dan fungsinya.
3) Lanal Palu segera menentukan tugas, fungsi dan tanggungjawab pejabat dan pengawak bidang keamanan siber dan IT (Administrator, Teknisi dan Operator beserta User lainnya yang terkait). Seperti Administrator memiliki tugas dan tanggungjawab

dalam bidang administrasi, mengawasi jaringan/*network*, melaksanakan pembinaan personel dalam bidang sistem keamanan siber dan IT, Teknisi memiliki tugas dan tanggungjawab sebagai pendukung teknis administrator, mengawasi sistem keamanan siber, serta melaksanakan pemeliharaan dan perbaikan terkait keamanan siber dan IT beserta perangkat pendukungnya. Operator adalah setiap personel baik prajurit TNI maupun PNS di lingkungan Lanal Palu yang memiliki tugas dan tanggungjawab dalam pengoperasian dan menggunakan komputer, perlu dibuat aturan yang ketat agar selain operator atau tidak setiap orang bisa mengakses dan menggunakan komputer di Lanal Palu.

4) Agar segera dibuat sistem jaringan LAN (*Local Area Network*) agar komputer-komputer Lanal Palu yang selama ini bekerja secara sendiri-sendiri (*stand alone*) dapat saling terintegrasi atau terhubung, sehingga semakin mudah pengawasannya dan akan semakin mudah dalam pembagian data (*data sharing*).
5) Personel atau sumber daya manusia yang berbakat menangani/membidangi sistem keamanan siber dan IT selama ini, dengan berbekal pengalaman dan pengetahuan yang minim serta belajar secara autodidak, agar diberikan kesempatan dalam berkarir, serta perlu dibina dan diberikan diklat (Pendidikan dan pelatihan) terkait teknologi keamanan siber dan IT terutama terkait adanya virus atau worm yang secara umum menyerang sistem komputer dan jaringan, seperti *Stuxnet* yang dapat mengambil alih sistem kontrol/kendali, serta *wannacry* yang dapat mengunci file dalam sistem komputer dan jaringan.
6) Agar pejabat dan pengawak sistem keamanan siber dan IT (Administrator, Teknisi dan Operator beserta personel terkait) diberikan Diklat (Pendidikan dan latihan) terkait pengetahuan dan praktek tentang system keamanan siber secara rutin, terjadwal dan berkelanjutan serta memiliki

rencana pengembangannya seiring dengan kemajuan teknologi yang semakin pesat dan cepat.

7) Sebagaimana diketahui bahwa saat ini komputer di Lanal Palu telah terhubung dengan Internet, sehingga perlu mendapat perhatian dan harus diwaspadai adanya ancaman dan serangan siber ke perangkat komputer-komputer melalui jaringan internet tersebut. Pengawak organisasi (administrator, teknisi dan operator) serta para user lainnya harus ekstra ketat dan jeli mengamati, mengontrol dan mengawasi anomali yang dapat terjadi pada komputer-komputer yang digunakan dalam instansi tersebut.
8) Personel atau sumber daya manusia Lanal Palu yang bertugas di bidang keamanan siber, baik yang bertugas sebagai administrator, teknisi, operator dan user lainnya, selain ditingkatkan dan dibekali pengetahuan dalam penggunaan komputer dan pengetahuan siber, agar ditingkatkan pengetahuan Bahasa inggrisnya karena dengan memiliki kemampuan Bahasa inggris dengan baik maka akan lebih mampu dan resisten terhadap ancaman/serangan keamanan siber, terlebih yang bersifat phising.
9) Lanal Palu agar melarang personel terhubung dan menggunakan jaringan internet kantor dengan menggunakan komputer dan perangkat pribadi lainnya. Bahwa komputer dan perangkat kantor benar-benar digunakan sesuai peruntukkannya untuk kegiatan dinas kantor saja. Konsekuensinya kantor harus melengkapi komputer dan perangkat kerja lainnya untuk mendukung tugas dan kegiatan operasional kantor.
10) Dalam menentukan jabatan dan pengawak organisasi di bidang keamanan siber Lanal Palu, agar menetapkan standar kualifikasi personel yang akan menduduki jabatan mulai dari jabatan sebagai perwira staf keamanan siber, kepala urusan administrasi, kepala urusan teknisi, dan kepala urusan operator beserta pengawak bidang keamanan siber lainnya.
11) Untuk pengawasan melekat (waskat) sangat penting diperhatikan dan dilaksanakan oleh pimpinan atau Komandan Lanal Palu kepada pejabat dan pengawak

organisasi keamanan siber dan IT, baik itu yang menjabat sebagai perwira staf keamanan siber, administrator, teknisi, dan operator beserta pengawak lainnya yang ada di dalam bidang keamanan siber, agar betul-betul diperhatikan terkait loyalitas dan integritasnya untuk instansi TNI AL, TNI dan untuk NKRI.

12) Melarang personel Lanal Palu untuk menggunakan dan terhubung ke dalam jaringan internet publik di tempat-tempat umum dengan menggunakan komputer atau perangkat milik kantor lainnya, hal ini sangat berisiko dan dapat membahayakan karena di tempat umum bisa menjadi tempat bagi peretas dan malware untuk melakukan aksi kejahatannya.
13) Lanal Palu agar membuat peraturan dalam penggunaan e-mail untuk kedinasan dan kegiatan operasional kantor menggunakan *e-mail* milik kantor.
14) Membuat peraturan dalam pengoperasian komputer, hanya personel yang ditunjuk saja yang diperbolehkan, dan itupun hanya diperbolehkan mengakses komputer yang hanya diperuntukkan secara khusus untuk dirinya sendiri sehingga dilarang untuk mengakses komputer milik personel/operator lainnya.
15) Membuat rencana kontigensi dan SOP dengan sejelas-jelasnya, agar dipahami dan dimengerti serta untuk dilaksanakan oleh seluruh pengawak bidang keamanan siber (administrator, teknisi, operator dan user), sehingga siapa yang berbuat apa akan sangat jelas, apabila ada tanda atau peringatan yang diberikan dapat berjalan dengan baik, efektif dan efisien serta sesuai dengan apa yang diharapkan dan direncanakan. Jika tiap-tiap personel paham dan mengerti terkait tugas dan tanggungjawabnya masing-masing dalam keamanan siber, maka proses pencegahan, penanganan dan pemulihannya akan lebih mudah dan cepat pengatasannya.
16) Menyiapkan ruangan atau tempat khusus "terbatas" yang tidak sembarang orang boleh masuk, yang boleh memasukinya hanya personel terkait atau tertentu saja, di pintu masuk dan didalam

ruangannya agar di pasang kamera cctv atau kamera pengawas dan dipastikan tetap berjalan dan berfungsi selama 24 jam penuh, agar bisa diketahui kegiatan atau aktivitas dan siapa saja yang ada dalam ruangan tersebut serta segala upaya dan niat kejahatan maupun sabotase tidak bisa terjadi.

17) Segera membuat *MoU* dengan pihak internet service provider (ISP) terkait dengan keamanan data dan kerahasiaan informasi, sebagai dasar untuk pertanggungjawabannya dalam bekerjasama dan menjamin kerahasiaan, keamanan data dan informasi.

18) Membuat aturan atau SOP terkait dalam pemusnahan komputer dan perangkatnya yang sudah tidak digunakan lagi.

b. Indikator *Hardware*

1) Segera membuat SOP terkait pengadaan barang dan jasa hardware/ komputer dan perangkatnya yang menjamin mutu, bergaransi dan tersertifikasi aman. Tujuannya untuk menjamin masa pakai hardware, selalu dalam keadaan siap dan kondisi prima serta tahan dan awet.

2) Meneruskan dan memperbaharui SOP terkait inventarisasi hardware dengan lebih terinci dan sedetail-detailnya, seperti spesifikasi peralatan dan kapan tanggal pembelian dan pemasangannya sehingga sangat jelas bisa diketahui masa pakainya, kapan hardware itu harus di upgrade dan diganti disesuaikan dengan kondisi kebutuhan kantor dan perkembangan teknologi yang ada.

3) Agar dalam pembangunan ruang / tempat server terjamin privasi, keamanan dan kenyamanannya serta dijaga dengan ketat oleh personel yang ditunjuk secara bergantian dan terjadwal dalam 24 jam penuh. Selain adanya *CCTV* atau kamera pengawas yang telah terpasang juga membuat pintu kaca dan tembok yang dapat dibuka dengan hanya menggunakan pin/kartu khusus serta sesuai standar dalam menjaga keamanan dan privasi.

4) Perlu segera dibentuk tim khusus terkait sistem sertifikasi yang dilaksanakan secara mandiri dan internal lingkungan TNI AL atau menunjuk badan jasa penyedia

keamanan data dan informasi yang terpercaya dan kredibel.

5) Perlu dibuat SOP bahwasanya webcamera pada perangkat komputer dan laptop milik mako Lanal Palu agar ditutupi apabila tidak sedang digunakan, karena webcamera dapat dijadikan sarana dalam memata-matai tanpa disadari oleh penggunanya.
6) Menjamin dan memastikan bahwa kabel optik yang dipasang dan menjalar dalam lingkungan kantor, koridor dan antar ruangan tidak terlihat dan tersembunyi dan aman dari ancaman baik dari pihak yang berniat jahat maupun aman dari gangguan hewan seperti tikus atau hewan lainnya, dan bila perlu dipasang *CCTV* atau kamera pengawas yang canggih pada setiap jalur yang dilintasi oleh kabel optik. Dalam pemasangan kabel optik juga sangat penting dipasang jaringan kabel optik cadangan yang dapat difungsikan apabila terjadi gangguan pada kabel optic utama bisa digantikan dan di switch dengan kabel optic cadangan.
7) Sistem kamera pengawas atau *CCTV* yang dipasang harus yang benar-benar sesuai dengan standard dan canggih, yang mampu mendeteksi berdasarkan dari bentuk wajah seseorang yang mengakses tanpa otorisasi, sistem yang mampu mendeteksi pihak yang tidak bertanggungjawab atau pihak eksternal yang memasuki daerah/ruang terbatas/terlarang seperti ruangan server.
8) Segera membuat server cadangan untuk antisipasi jika terjadi serangan siber seperti virus/worm dan server yang utama berhasil dilumpuhkan, untuk itu sangat penting disiapkan perangkat computer yang khusus dengan memiliki spek yang tinggi sehingga dapat berperan dan berfungsi sebagai server untuk menggantikan sementara server utama apabila terjadi serangan dan melumpuhkan server utama, server cadangan tidak terkoneksi dengan server yang utama, computer server cadangan ini nantinya akan berperan dan berfungsi dalam melakukan *system data recovery* pada komputer client dan sekaligus membersihkan dari *virus/worm*. Namun jaringan ini sifatnya

sementara dan apabila server utama sudah bisa aktif kembali, secara otomatis jaringan cadangan ini akan dinonaktifkan selanjutnya melaksanakan pengecekan dan memastikan serangan virus yang terjadi tidak menginfeksi perangkat server cadangan tersebut.

9) Segera menyiapkan dan menyimpan system backup pada harddisk eksternal dengan system backup pada computer yang memiliki system oprasi yang tidak sama.
10) Melarang secara penuh tamu kantor maupun personel terkait lainnya dalam menggunakan jaringan internet dan wifi di kantor untuk keperluan pribadinya, jaringan internet untuk umum perlu disediakan tersendiri dalam menghindari perpindahan *malware*.
11) Melaksanakan dan memastikan pensettingan komputer Mako sampai dengan ke endpoint, hal tersebut guna memudahkan dalam memonitor computer yang beroperasi di lingkungan Mako.
12) Menyiapkan pencadangan *hardware* / perangkat keras disesuaikan dengan tingkat yang paling sering mengalami kerusakan, gangguan atau yang memegang peran dan fungsi paling penting dan essensial dalam menjaga kelancaran operasional jaringan (server) sebagai contoh kabel optic, harddisk dan lain sebagainya disesuaikan dengan kondisi dan kebutuhan dilapangan. Hal tersebut untuk menjaga agar jaringan tidak mengalami gangguan dan terjamin selalu aktif.
13) Melaksanakan pembaruan hardware secara berkala dan merata dan diatur dalam SOP, misalnya setiap 3 tahun sekali, hal tersebut guna menjamin dan menjaga kelancaran dan keamanan operasional kegiatan sehari-hari dari ancaman/serangan siber.
14) Membuat SOP terkait keharusan dalam pengadaan hardware/perangkat keras dengan menggunakan yang original dan terjamin kualitasnya.

c. **Indikator *Software***

1) Membuat SOP terkait kewajiban agar seluruh personel terkait menggunakan software dan aplikasi yang original dan berlisensi serta bukan *crack*-an. Hal tersebut terkait dengan hak cipta dan terjaminnya kualitas software yang digunakan

bebas dari virus yang bisa mengancam system keamanan siber, computer dan jaringan, dan apabila personel tidak menggunakan software yang tidak original dan tidak berlisensi akan sangat berisiko adanya intrusi malware ke perangkat komputer menjadi lebih tinggi.

2) Membuat SOP terkait program pembaruan atau update software system operasi atas aplikasi secra terjadwal dan berkala pada computer server maupun client. Dengan menggunakan system operasi dan aplikasi yan original, jika ada fitur pembaruan akan selalu diberitahukan dengan pesan tersedia pembaruan dan si produsen juga akan selalu melindungi kliennya. Update pembaruan software juga dipastikan tersedia jika baru saja atau telah terjadi adanya serangan siber secara global, dengan tidak menunggu waktu yang lama para produsen system operasi, antivirus maupun aplikasi langsung membuat dan memberikan update terbarunya agar perangkat lunak kebal/resisten dari virus tersebut.

3) Agar tidak menggunakan *software* (sistem operasi, aplikasi) yang dirilis dibawah 5 (lima) tahun, sebisa mungkin komputer dan perangkat computer maupun software agar menyesuaikan perkembangan teknologi yang ada dan terupdate, semakin sering mengupdate software akan diikuti juga kebutuhan spesifikasi perangkat hardware nya sehingga kinerja komputer, performa dan keamanannya juga akan semakin lebih baik, hal tersebut untuk meminimalisir kerentanan terhadap ancaman dan serangan siber.

d. **Indikator *Infrastructureware***

1) Selain adanya penjagaan yang selama ini sudah terlaksana oleh prajurit Lanal Palu selama 24 jam penuh, perlu menambah kamera pengawas pada jalur kabel optik dan titik-titik yang dianggap rawan untuk menjaga dan mendeteksi serta untuk mencegah pihak-pihak yang tidak bertanggungjawab dan berniat jahat serta adanya sabotase.

2) Agar menambah pengamanan dengan menambah system pendeteksi drone dan system penangkal drone, dengan adanya

pemasangan system tersebut dengan harapan serangan/ancaman udara dapat dicegah dan diminimallisir.

3) Segera membuat *MoU* dan komitmen terkait keamanan data dan informasi dengan *internet sistem provider (ISP)* yang telah menjadi langganan Lanal Palu.
4) Membuat SOP untuk melakukan pencadangan perangkat/hardware dalam menjaga kemampuan dan kehandalan infrastruktur jaringan, antara-lain kabel optic, pemancar wifi, komputer/perangkat cadangan yang mampu berperan sebagai server dan perangkat terkait lainnya.

e. **Indikator *Firmware***

1) Segera membentuk satuan kerja yang khusus memiliki tugas dan tanggungjawab di bidang keamanan siber dan *IT*. Hal tersebut sangat penting sebagai dasar yang akan mewadahi terkait kebijakan, rencana dan program pelaksanaan, serta evaluasi dalam peningkatan keamanan siber kedepan di instansi Lanal Palu.
2) Membuat SOP dalam membuat dan merencanakan roadmap/peta jalan arah kebijakan organisasi dalam keamanan siber. Dalam pembuatan roadmap akan lebih baik melibatkan pihak-pihak terkait yang ahli di bidangnya, berpengalaman dan berkompeten, sebagai contoh Kemeninfokom, BSSN, Pushansiber Kemhan, Satsiber TNI, Perguruan Tinggi dan lain sebagainya.
3) Membuat SOP terkait penanganan *Remote Data Center* dan *Data Recovery*, hal tersebut sangat penting dalam mencegah dan mengantisipasi rusak atau hilangnya data akibat serangan malware, dan menjaga dari kemungkinan bencana alam gempa bumi, kebanjiran, kebakaran atau juga dari kemungkinan aksi vandalism yang bisa terjadi di mako Lanal Palu.

f. **Indikator *Budgetware***

1) Segera memulai dan merencanakan anggaran untuk program terkait keamanan siber. namun hal ini baru akan dapat berjalan setelah satuan keamanan siber secara resmi terbentuk. Dalam merencanakan program kerja dan anggaran kedepan harus secara jeli dan prediktif disesuaikan dengan kondisi dan perkembangan di masa yang akan datang.

2) Memprioritaskan penganggaran terkait dengan kebutuhan perangkat hardware dan software yang paling terpenting dahulu, seperti pengadaan perangkat/komputer dalam menggantikan laptop bagi personel Lanal Palu yang masih menggunakan perangkat milik pribadi. Hal ini untuk meminimalisir kerentanan intrusi malware.
3) Segera merencanakan penyiapan anggaran untuk program Pendidikan dan Latihan (Diklat), kursus-kursus, sosialisasi dan sebagainya terkait program keamanan siber dan IT bagi personel Lanal Palu, guna menambah pengetahuan dan meningkatkan awareness personel tersebut dalam bidang keamanan siber.
4) Segera merencanakan dan penyiapan program kerja dan anggaran guna meningkatkan kapabilitas dan kapasitas peralatan dan perangkat komputer beserta jaringannya di lingkungan Mako Lanal Palu.

Urgensi pertahanan siber ditujukan untuk mengantisipasi datangnya ancaman dan serangan siber yang terjadi dan menjelaskan posisi pertahanan saat ini, sehingga diperlukan kesiapan dan ketanggapan dalam menghadapi ancaman serta memiliki kemampuan untuk memulihkan akibat dampak serangan yang terjadi di ranah siber (syamsudin A, 2014).

Kesimpulan dan Saran

kondisi sistem pertahanan siber berbasis *Six-Ware Cyber Security Framework* di Mako Lanal Palu disimpulkan bahwa berdasarkan analisis kualitatif Lanal Palu belum siap dan belum mampu dalam menangani adanya serangan/ancaman siber, sedangkan berdasarkan analisis kuantitatif secara umum bahwa kemampuan teknologi pertahanan siber berbasis *Six-Ware Cyber Security Framework* di Mako Lanal Palu dalam menghadapi ancaman siber dalam kategori baik. Secara keseluruhan disimpulkan bahwa Lanal Palu telah memiliki teknologi, namun belum memiliki rencana pengembangan pembangunan teknologi pertahanan keamanan sibernya.

Mako Lanal Palu dalam pembangunan teknologi pertahanan

keamanan siber berbasis *sixware cyber security defence framework,* semua indikator dalam SWCS harus diperhatikan mulai dari *brainware, hardware, sofware, infrastuctureware, firmware* dan *Budgetware*. Dari kedua analisis diintepretasikan bahwa semua faktor dalam SWCS sangat berpengaruh dan semua faktor tersebut harus adaptif.

Segera mengusulkan pembentukan struktur organisasi (peta jabatan) bidang keamanan siber dan IT, diikuti penyediaan SDM/personel bidang keamanan siber dan IT serta merencanakan program kerja dan anggarannya, sehingga implementasi SWCS di Lanal Palu siap dalam menghadapi ancaman/serangan keamanan siber, agar kerangka SWCS dapat diimplementasikan di Lanal Palu dan dapat dibuktikan portabilitasnya, sehingga kerangka kerja tersebut dapat dipandang layak untuk ditingkatkan ke dalam bentuk aplikasi agar portabilitasnya lebih meningkat. Sebagai alat pertahanan negara wilayah strategis di wilayah kerja propinsi Sulawesi Tengah, Lanal Palu harus meningkatkan sinergitas antar berbagai instansi pemerintah, perusahaan swasta dan perguruan tinggi atau lembaga pendidikan terkait, terhadap keamanan dalam bidang siber dan *IT* guna menjaga dan meningkatkan Sistem Pertahanan Negara.

Daftar Pustaka

Ardiyanti, H. (2014). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Politica*, *5*, 95–110.

BSSN. (2020). *Rekap Serangan Siber (Januari – April 2020)*. Jakarta. https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

Creswell, J. W. & Clark, V. L. P. (2018). *Designing and Conducting Mixed Methods Research*. SAGE Publications, Inc. All.

Dewi. (2020). *BSSN Catat Adanya 88,4 Juta Serangan Siber Selama Pandemi Corona Artikel ini telah tayang di Kompas.com dengan judul "BSSN Catat Adanya 88,4 Juta Serangan Siber Selama Pandemi Corona", Klik untuk baca: https://www.kompas.com/tren/read/2020/04/23/165400665*. Kompas.Com. https://www.kompas.com/tren/read/2020/04/23/165400665/bssn-catat-adanya-88-4-juta-serangan-siber-selama-pandemi-corona?page=all#:~:text=KOMPAS.com - Pusat Operasi Keamanan,1 Januari-12 April 2020

Gemilang Gultom, R. A., Kustana, T., & Oktovianus Bura, R. (2018). Enhancing Computer Network Security Environment By Implementing the Six-Ware Network Security Framework (Swnsf). *ResearchGate*, *December 2018*, 153–166.

https://doi.org/10.5121/csit.2018.81714

Gultom, R A G, Farid, A., Lestari, A. A., Lahallo, C. A. S., & Akbar, R. N. (2020). Cyber-Based Defense Technology Development of the Six-ware Cyber Framework to Enhance the Implementation of the National Defense System in the City of Batam. *International Journal of Advanced Science and Technology*, *29*(7), 3431–3436. http://sersc.org/journals/index.php/IJAST/article/view/17631

Gultom, Rudy Agus Gemilang, & Alrianto, B. (2016). Enhancing Network Security Environment by Empowering Modeling and Simulation Strategy. *The Eleventh International Conference on Internet Monitoring and Protection Enhancing*, *c*, 45–52.

Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Times*, *5*(2), 35–42. http://stmik-time.ac.id/ejournal/index.php/jurnalTIMES/article/viewFile/556/126

maharani, tsarina. (2020). *Situs Web Diretas, DPR Diubah Menjadi "Dewan Pengkhianat Rakyat" Artikel ini telah tayang di Kompas.com dengan judul "Situs Web Diretas, DPR Diubah Menjadi 'Dewan Pengkhianat Rakyat'", Klik untuk baca: https://nasional.kompas.com/read/2020/10/08/10162531/*. Kompas.Com. https://nasional.kompas.com/read/2020/10/08/10162531/situs-web-diretas-dpr-diubah-menjadi-dewan-pengkhianat-rakyat

Putra, D. A., Saragih, H. J. R., & Deksino, G. R. (2020). the Ministry of Defence Risk Management Implementation To Support the Country ' S Defense. *Manajemen Pertahanan*, *6*(1), 100–121.

Putra, R. D., & Deni, D. A. R. (2018). Ancaman siber dalam persfektif pertahanan negara (studi kasus sistem pertahanan semesta) siber threats in state defense persfectives (total defense system case study). *Jurnal Prodi Perang Asimetris*, *4*, 99–120.

Riza, H. (2017). *Jaga Kedaulatan Nasional, Cyber Defense TNI Perlu Diperkuat*. Jakarta. https://www.bppt.go.id/teknologi-informasi-energi-dan-material/2982-jaga-kedaulatan-nasional-cyber-defense-tni-perlu-diperkuat

Sa'diyah, N. K., & Vinata, R. T. (2016). Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara. *Perspektif*, *21*(3), 168. https://doi.org/10.30742/perspektif.v21i3.587

sugiyono. (2017). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung*. CV. Alfabeta.

Sujarweni, V. W. (2020). *SPSS Untuk Penelitian*. Pustaka Baru Press.

syamsudin A. (2014). *Pedoman Pertahanan Siber* (1 st Ed (ed.); 1st ed.). Kementrian Pertahanan Republik Indonesia.