Jurnal Peperangan Asimetris
Volume 8, Nomor 1 2022 E-ISSN 2830-0475

# PERTAHANAN SIBER INDONESIA DI KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA

***INDONESIA'S CYBER DEFENSE STRATEGY AT THE MINISTRY OF DEFENSE OF THE REPUBLIC OF INDONESIA***

Nur Arifina
Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan,
Universitas Pertahanan Republik Indonesia,
arifina68@gmail.com

**Abstrak –** Pusat Pertahanan Siber yang dikenal dengan singkatan Pus Han Siber merupakan instansi pelaksana tugas dan fungsi dari Badan Instalasi Strategis Pertahanan yang memiliki tugas dalam melaksanakan tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber. Pada setiap tahun nya selalu terjadi peningkatan pada permasalahan serangan siber seperti *phising* (pengelabuhan), *malware*, *ransomware, spam* dan lain-lain. Peneliti mengkaji bagaimana strategi pertahanan siber Indonesia dalam di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia. Penelitian menggunakan metode kualitatif. Peneliti melakukan wawancara kepada beberapa narasumber dan studi literatur yang memiliki keterkaitan dengan obyek penelitian. Dan wawancara yang tentu nya sudah di tentukan oleh peneliti untuk mendapatkan sebuah data. Sedangkan data sekunder didapatkan dari dokumentasi berupa gambar dan dokumen tertulis yang memiliki keterkaitan dengan strategi Pushansiber dalam menghadapi ancaman siber. 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. Maka dapat disimpulkan bahwa strategi pertahanan siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia dengan menjalankan Peraturan Menteri Pertahanan Republik Indonesia No. 82 Tahun 2014 terkait pedoman pertahanan siber menjadikan acuan yang bertujuan untuk meningkatkan kapabilitas dan selaras dalam membangun sistem siber pada sektor sumber daya manusia, perangkat keras, perangkat lunak, infrastruktur, firmware dan anggaran.

**Kata Kunci** : Pushansiber, Strategi, Keamanan Pertahanan Siber, Pertahanan Siber, Kementerian Pertahanan Republik Indonesia.

***Abstract*** *– The Cyber Defense Center known by the abbreviation Pus Han Siber is an implementing agency of duties and functions of the Defense Strategic Installation Agency that has a duty in carrying out governance, cooperation, operations, and cybersecurity assurance. In every year there is always an increase in the problem of cyber attacks such as phishing, malware, ransomware, spam and others. Researchers examined how Indonesia's cyber defense strategy in cyber systems at the Cyber Defense Center of the Ministry of Defense of the Republic of Indonesia. Research uses qualitative methods. Researchers conduct interviews with several sources and literature studies that have links to research objects. And the interview has certainly been determined by researchers to get a data. While secondary data is obtained from documentation in the form of images and written documents that have links to Pushansiber's strategy in cyber systems to deal with cyber threats. Pushansiber uses strategies to improve cyber system capabilities that take time. Then Pushansiber has also created and entered on a strategy plan from 2020-2024. It can be concluded that Indonesia's cyber defense strategy at the Cyber Defense Center of the Ministry of Defense of the Republic of Indonesia by implementing The Minister of Defense Regulation of the Republic of Indonesia No. 82 of 2014 related to cyber defense guidelines makes references aimed at improving capabilities and aligned in building cyber systems in the human resources sector, hardware, software, infrastructure, firmware and budget.*

**Keywords**: *Pushansiber, Strategy, Cybersecurity, Cyber Defense, Ministry of Defense of the Republic of Indonesia.*

## Pendahuluan

Globalisasi memainkan peran penting yang dapat memberikan perubahan pesat dalam kemajuan teknologi dan perubahan dari cara pandang manusia yang ke arah modern. Perkembangan teknologi dan infromasi memberikan pengaruh pada sistem informasi intelijen yang menjadikan sebuah ajang dalam keunggulan informasi, strategi, taktik, kebijakan dan kegiatan intelijen guna meningkatkan kekuatan dalam peperangan informasi intelijen. Peperangan dalam dunia siber masuk kedalam kategori peperangan asimetris.

Kehidupan yang modern ini telah mengalami perubahan pengembangan dan peningkatan pada ilmu pengetahuan dan digitalisasi teknologi informasi dan

komunikasi menjadi lebih cepat dan maju. Munculnya teknologi komputer dapat membawa dampak besar bagi umat manusia dan memberikan kontribusi yang sangat signifikan untuk dapat menyelesaikan berbagai hal dengan cepat dan efektif. Selain dari kegiatan dari teknologi komputer, yang mana file tersimpan pada komputer, internet dan ponsel sangat rentan terhadap adanya peretas dalam segala bentuk cara dalam mengakses yang tidak sah pada dunia maya. Maka dari itu diperlukan adanya kemanan dunia pada sistem informasi yang efisien dan kuat.

Dengan adanya internet yang dapat menghasilkan komunikasi dan dapat juga menghasilkan perang siber yang dapat mengancam pertahanan negara. Perang pada di dunia siber telah memakai jaringan komputer yang membentuk suatu strategi pertahanan atau penyerangan pada sistem informasi dari lawan. Pemanfaatan teknologi dapat dilakukan oleh orang-orang yang tidak bertanggung jawab untuk dapat mengganggu, merusak, menguasai dan menghentikan jalannya informasi dan data yang memberikan kerugian dan menghancurkan si lawan.

Dari adanya perubahan tersebut dapat dilihat adanya kekuatan pada keunggulan informasi yang dilakukan oleh tiap-tiap negara. Teknologi pada masa sekarang tidak hanya berbentuk alutista saja, bahkan dapat memanfaatkan penggunaan teknologi yang dapat merusak fisik pada perang siber. Ancaman serangan siber dapat memberikan dampak pada mengganggu pertahanan suatu negara. Ancaman juga merupakan tindakan yang jahat guna merusak dan mencuri data atau bahkan dapat mengganggu suatu atau seluruh sistem organisasi.

Kejahatan pada dunia siber menjadikan tolak ukur ancaman yang serius di seluruh dunia. Clare (2021) menjelaskan bahwa pada setiap tahun nya selalu terjadi peningkatan pada permasalahan serangan siber seperti *phising* (pengelabuhan), *malware*, *ransomware, spam* dan lain-lain. Dibawah ini akan menjelaskan mengenai

Kondisi di dunia terhadap adanya serangan siber yang telah terjadi dalam *Norton* dan *Center for Strategic International Studies* :

**Tabel 1 Kondisi di dunia dengan adanya serangan siber**

| No | Serangan Siber | Tahun |
|---|---|---|
| 1 | Adanya 75% serangan siber yang ditargetkan dengan menggunakan email | 2020 |
| 2 | Serangan siber cenderung menggunakan jet F-35 daripada dengan menggunakan rudal | 2020 |
| 3 | FBI menerima pengaduan sebanyak 15.421 dengan adnya kejahatan penipuan di internet | 2020 |
| 4 | Adanya peningkatan serangan *ransomware* mencapai 102% | 2021 |
| 5 | Rusia menargetkan dan memblokir aplikasi "pemungutan suara cerdas" yang dibuat oleh Kremlin Alexei Navalny | 2021 |
| 6 | Adanya serang siber yang memanfaatkan kondisi Covid-19 pada situs vaksin untuk menutup penjadwalan di wiliayah Italia Lazio | 2021 |
| 7 | Kementerian Pertahanan Ukraina mengklaim adanya situs angkatan laut yang telah di targetkan oleh *Hacker* Rusia untuk dapat menerbitkan laporan palsu mengenai *Sea Breeze*-2021 latihan militer internasional | 2021 |
| 8 | FBI dan Pusat Keamanan Siber Australia telah melakukan peringatan kepada Avaddon yang telah menargetkan kampanye militer *ransomware* dengan menargerkan negara Australia, Belgia, Kanada, Cina, Kosta Rika, Republik Ceko, Perancis, Jerman, India, Indonesia, Italia, Yordania, Peru, Polandia, Portugal, Spanyol, UEA, Inggris dan Amerika Serikat di bidang: akademisi, konstruksi, maskapai penerbangan, energi, pemerintah, kesehatan, konstruksi, peralatan, keuangan, dan lain-lain | 2021 |

Tabel 1 Sumber: diolah peneliti 2022

Tabel 1 menunjukkan bahwa antara tahun 2020-2021 telah terjadi ancaman serangan siber di dunia dengan kategori mengkahawatirkan. Pasalnya, dengan kurun waktu 1 tahun, terdapat banyak nya serangan siber yang dapat merugikan dan

mengganggu tiap-tiap negara. Maka ini diperlukan adanya perhatian, kewaspadaan dan antisipasi dengan adanya ancaman siber.

Tak luput Indonesia juga telah menjadi target penyerangan siber yang dilakukan oleh peretas dari luar dan dalam negeri. Seperti kondisi serangan siber yang didapati oleh negara Indonesia, yaitu Serangan yang dilakukan oleh penyusupan siber dan penyalahgunaan pada protokol komunikasi dapat menjadi ancaman yang harus diwaspadai penuh. Apabila tidak melakukan antisipasi secara dini, kegiatan tersebut dapat merusak, merubah, mencuri, menghancurkan dan melumpuhkan suatu sistem informasi di suatu negara. Seperti tabel di bawah ini yang menjelaskan serangan siber yang telah terjadi di Indonesia mulai dari tahun 2017-2021:

**Tabel 2 Kondisi di Indonesia dengan adanya serangan siber (2017-2021)**

| Tahun | Jumlah Inseden Serangan Siber | Jenis Serangan |
|---|---|---|
| 2017 | 205.502.159 juta | *Defacement Web, Malware,* dll |
| 2018 | 232.497.974 juta | *Defacement Web, Malware, Phishing,* dll |
| 2019 | 290.000.000 juta | *Malware, Phishing, and Ransomware,* dll |
| 2020 | 495.000.000 juta | *Malware, Phishing, Data Leak and Ransomware,* dll |
| 2021 | 1.300.000.000 miliar | *Malware, Phishing, Data Leak and Ransomware,* dll |

Tabel 2 Sumber: diolah peneliti 2022

Menurut Anjani (2021) menjelaskan bahwa pada tahun 2019 terdapat kejahatan siber yang memberikan kerugian sebanyak US$ 34,2 miliar di Indonesia dan dengan ditambah kondisi pandemi Covid-19 yang menyebabkan peningkatan pada serangan siber yang jenisnya seperti *phising, malware spams* dan ransomware.

Mahendri (2021) menjelaskan bahwa Adanya peretas yang telah menyerang pada situs website dari Sekolah Staf dan Komando Angkatan Darat (Seskoad) yang bersatatus *under maintenance.*

Makmur (2014) menjelaskan bahwa mengatakan mengenai ilmu pertahanan menjadi suatu ilmu yang berasal dari strategi, Ilmu militer dan ilmu &ilmu seni perang. Handrini(2016) menjelaskan bahwa terdapatnya beberapa masalah dalam pembangunan keamanan *cyber* di suatu negara seperti terdapatnya kurang penanganan dalam penyerangan siber. Rudy Gultom (2018) menjelaskan bahwa mengenai *Six-ware Network Security Framework* (SWNSF) adanya 6 unsur dalam membangun sistem siber dan keamanan negara dalam bidang teknologi informasi di dunia siber guna menjaga pertahanan negara, seperti:

a. Manusia (*Brainware*),
b. Perangkat Keras (*Hardware),*
c. Perangkat Lunak (*software),*
d. Infrastruktur (*infrastructure),*
e. *Firmware*
f. Anggaran (*budgeting)*

Berdasarkan dari latar belakang masalah yang telah di kemukakan di atas, peneliti mengangkat permasalah yang sedang terjadi sebagai bahan penilitian. Selanjutnya peneliti menjadikan karya tulis ilmiah ini dalam bentuk tesis dengan judul "Strategi Pertahanan Siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia"

**Metode Penelitian**

Penelitian ini akan dilakukan dengan menggunakan pendekatan metode kualitatif, yang bertujuan untuk dapat mencari, menganalisis dan mengelola dari peristiwa langsung di lapangan dengan menginterpretasikan interaksi sosial dengan

menggunakan wawancara dan observasi. Menurut Sugiyono (Sugiyono, 2018), penelitian kualitatif berlandaskan pada filsafat, yang digunakan untuk meneliti pada kondisi ilmiah (eksperimen) yang aman si peneliti menjadi instrumen, teknik dalam pengumpulan data dan dianalisi yang bersifat kualitatif lebih menekankan pada maksudnya atau makna.

Berdasarkan latar belakang yang ada, maka peneliti membuat rumusan masalah yaitu, sebagai berikut:

a. Bagaimana faktor-faktor kendala dalam membangun sistem siber guna menghadapi ancaman siber?
b. Bagaimana strategi pertahanan siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia dalam meningkatkan kapabilitas pada sistem siber?

**Teknik Pengumpulan Data**

Teknik pengumpulan data pada penelitian ini dimulai dari menganalisis bagaimana strategi pertahanan siber dalam membangun sistem siber dalam menghadapi ancaman siber. Teknik pengumpulan data dapat dilakukan dengan *interview* (wawancara), observasi (pengamatan) dokumentasi. Moleong (2012) menjelaskan bahwa mengatakan bahwa Pengumpulan data bisa memakai sumber data primer (sumber data yang memberikan data langsung kepada peneliti), dan sumber data sekunder (data yang diberikan tidak langsung kepada peneliti yang mana menggunakan perantara).

**Pusat Pertahanan Siber (Pus Han Siber)**

Pusat Pertahanan Siber yang dikenal dengan singkatan Pus Han Siber merupakan instansi pelaksana tugas dan fungsi dari Badan Instalasi Strategis Pertahanan Kemhan dikepalai oleh Kepala Pusat Pertahanan Siber (Kapus Han Siber) yang memiliki tugas

dalam melaksanakan tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber

**Hasil dan Pembahasan**

Pada tahap pengolahan data ini, peneliti telah melakukan pemeriksaan atas jawaban dari hasil beberapa informan dan telah mengelompokkan jawaban yang sesuai dengan pertanyaan penelitian. Miles dan Huberman (2014) menjelaskan bahwa Proses tersebut disebut dengan kondensasi data dari kondensasi data ini yang mengarah pada hal yang penting.

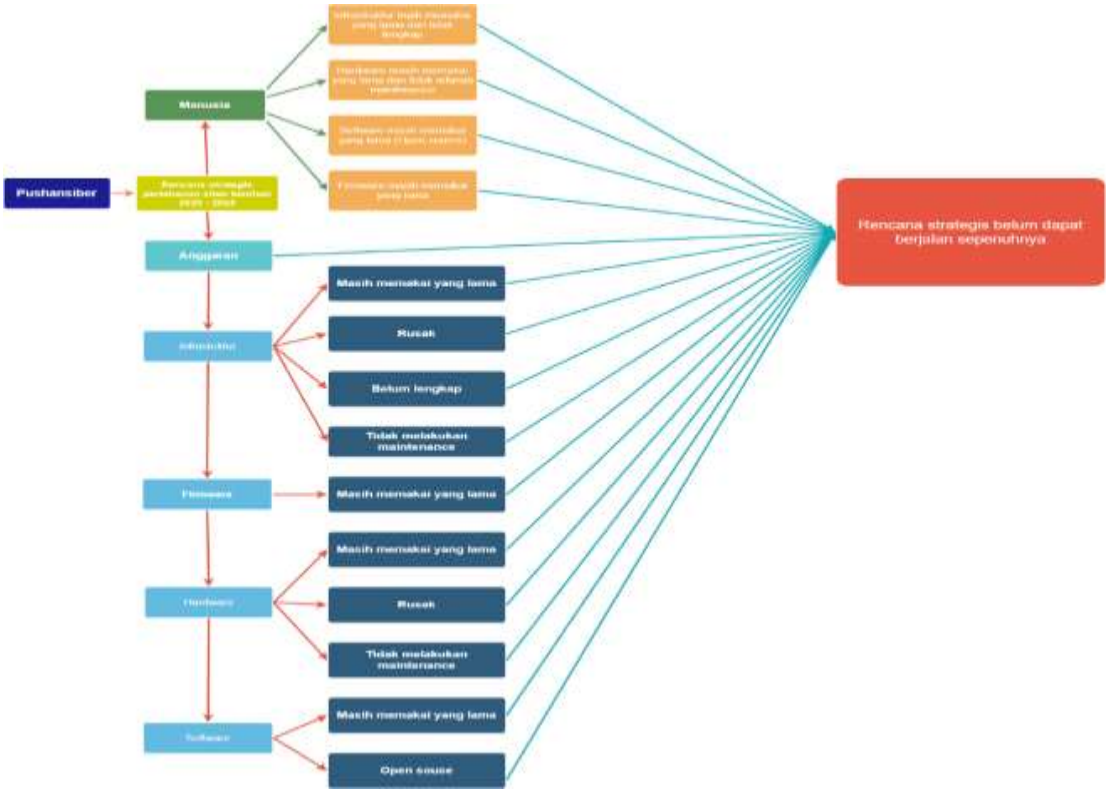
**Hasil Analisis Data**

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*).

**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.

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

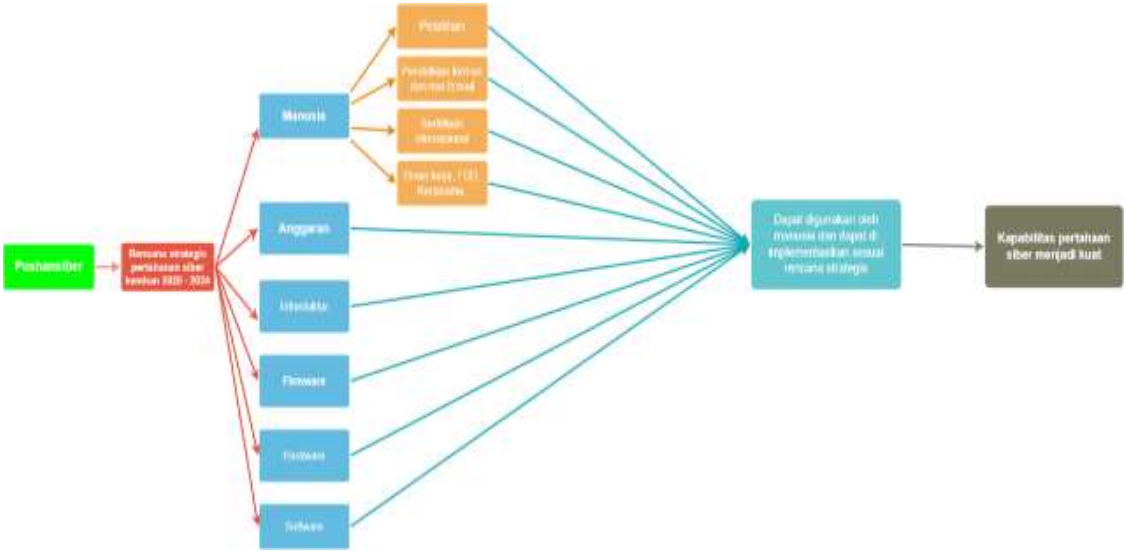



**Gambar 1 Faktor-faktor kendala dalam membangun sistem siber di Pushansiber**

**Sumber: diolah peneliti 2022**

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

Kementerian Pertahanan (2015) menjelaskan bahwa 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. Pushansiber selalu berupaya untuk kuat agar nantinya dapat menjaga dan melindungi terhadapa 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.




**Gambar 2 Strategi Pertahanan Sibebr di Pushansiber Dalam Meningkatkan Kapabilitas Sistem Siber**

**Sumber: diolah peneliti 2022**

**Kesimpulan Rekomendasi dan Pembatasan**

Kesimpulan yang peneliti dapatkan selama melakukan penelitian mengenai Strategi Pertahanan Siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia, adalah dari pertanyaan penelitian dari rumusan masalah mengenai "faktor-faktor kendala dalam membangun sistem siber guna menghadapi ancaman siber" dan pertanyaan yang kedua dari rumusan masalah mengenai "strategi pertahanana siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia" peneliti telah mendapatkan jawaban dari pertanyaan penelitian yang telah dijelaskan di bawah ini sebagai berikut:

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

Penulis telah mendapatkan hasil analisis mengenai terdapatnya faktor-faktor kendala sistem siber yang dapat menghambat kemampuan kinerja dari Pushansiber.

Dapat dilihat faktor kendala yang terbesar di Pushansiber adalah anggaran dan sumber daya manusia. Pemerintah belum memberikan perhatian yang serius dalam memberikan anggaran khusus untuk siber.

Pada teori SWNSF perlu dilakukan pembangunan dan pengembangan kembali untuk dapat meningkatkan dan memperkuat sistem pertahanan siber. Posisi Pushansiber masih dalam posisi lemah dalam sektor sistem siber yang dikarenakan banyaknya faktor kendala yang dimiliki. Dan paada teori keamanan jaringan sistem juga masih sangat lemah karena belum adanya dukungan anggaran dari pemerintah untuk dapat membeli *software* untuk dapat melakukan pengamanan yang mutakhir guna menghadapi ancaman dan serangan siber yang ada.

**Strategi Pertahanan Siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia Dalam Meningkatkan Kapabilitas Pada Sistem Siber**

Berdasarkan dari hasil penelitian dan juga pembahasan yang sudah di uraikan pada diatas, maka dapat disimpulkan bahwa strategi pertahanan siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia dengan menjalankan Peraturan Menteri Pertahanan Republik Indonesia No. 82 Tahun 2014 terkait pedoman pertahanan siber menjadikan acuan yang bertujuan untuk meningkatkan kapabilitas dan selaras dalam membangun sistem siber pada sektor sumber daya manusia, perangkat keras, perangkat lunak, infrastruktur, frimware dan anggaran. Saran untuk pemerintah agar dapat menyalaraskan regulasi dan peraturan untuk dapat menerima sumber daya manusia yang non organik dan bukan anggota TNI.

**Daftar pustaka**

Anjani, N. (2021). Perlindungan Keamanan Siber di Indonesia. https://c95e5d29-0df6-4d6f-8801-

1d6926c32107.usrfiles.com/ugd/c95e5d_287e77235dd64648bedf3ec06952d521.pdf , diakses pada 07 Januari 2022.

Handrini, A. (2016). Keamanan *Cyber* dan Tantangan Pengembangannya Di Indonesia. https://jurnal.dpr.go.id/index.php/politica/article/view/336/270 , diakses pada 10 Januari 2022

Kementerian Pertahanan Republik Indonesia. (2015). Buku Putih Pertahanan Indonesia. Jakarta:.

Clare, S. (2021). 115 cybersecurity statistics and trends you need to know in 2021. Retrieved from https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html

Gultom, R A. (2018). *Enhancing Computer Network Security Environment By Implementing The Six-Ware Network Security Framework (SWNSF)*. Bogor: Indonesia Defense University

Mahendra, C. (2021). Situs Resmi Seskoad Di-Hack, Pemerintah Harus Benahi Keamanan Siber. Retrieved from https://www.cloudcomputing.id/berita/situsresmi-seskoad-di-hack-pemerintah-harus-benahi-keamanan-siber

Miles, M. B., Huberman, & Saldana, J. (2014). *Qualitative Data Analysis, A. Methods Sourcebook, Edition 3. N*. New York: Sage Publications

Moleong, L. J. (2012). Metodologi Penelitian Kualitatif. Bandung: PT. Remaja Rosdakarya

Supriyatno, M. (2014). *Ilmu Pertahanan.* Jakarta: Yayasan Pustaka Obor Indonesia

Sugiyono, S. (2018). Metode Penelitian Kuantitatif, Kualitatif dan R&D. Bandung: Alfabet