e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 9 No 6 Tahun 2022 Hal. : 2218-2227

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

available online http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

STRATEGI PERTAHANAN SIBER INDONESIA DI PUSAT PERTAHANAN SIBER KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA

Nur Arifina[1)], Fazar Sidik[2)], Rudy Sutanto[3)]

[1)] Universitas Pertahanan Republik Indonesia, Fakultas Strategi Pertahanan, Program Studi Peperangan Asimetris

[2)] Universitas Budi Luhur, Fakultas Teknik Sistem Informasi, Program Studi Magister Ilmu Komputer

[3)] Universitas Pertahanan Republik Indonesia, Fakultas Strategi Pertahanan, Program Studi Peperangan Asimetris

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.

*Correspondence Address : arifina68@gmail.com, fajarsidik1430@gmail.com
DOI : 10.31604/jips.v9i6.2022.2218-2227

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

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

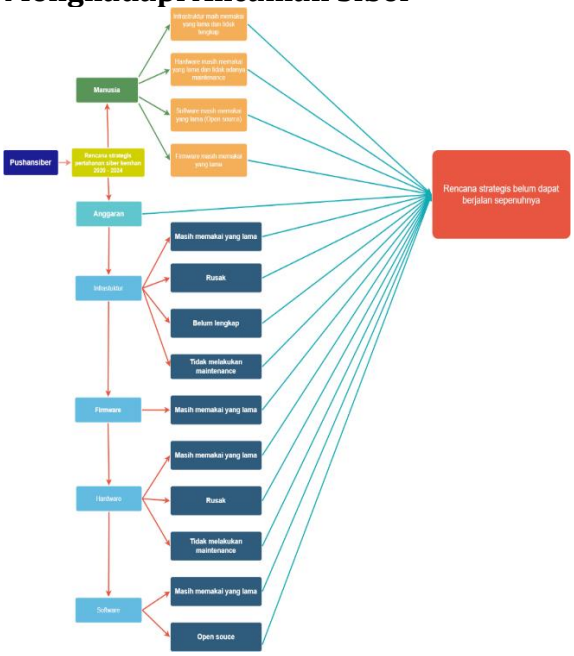
HASIL DAN PEMBAHASAN

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.

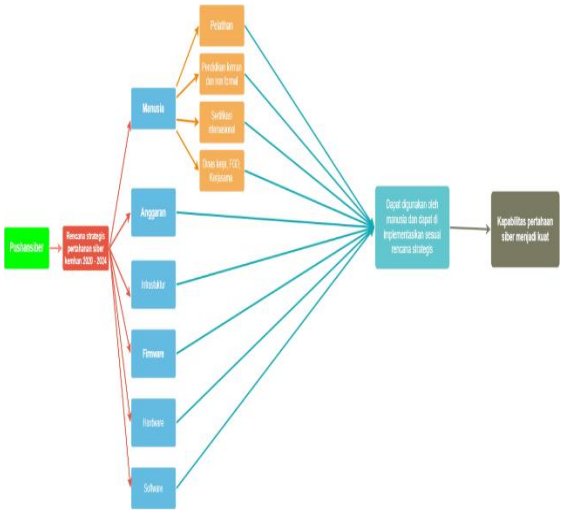
Faktor-Faktor Kendala Dalam Membangun Sistem Siber Guna Menghadapi Ancaman Siber



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

SIMPULAN

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.

A. Rekomendasi Teoritis

Berbasis dari hasil penelitian dan kesimpulan di atas, peneliti memberikan beberapa saran kepada pemerintah, masyarakat dan peneliti selanjutnya, seperti:

1. Kepada akademisi / peneliti selanjutnya disarankan untuk dapat melakukan penelitian lebih lanjut mengenai strategi pembangunan, pengembangan dan penguatan sistem siber dalam perguruan tinggi.
2. Kepada pemerintah untuk melindungi dan menjaga agar segera membuat dan menerapkan langsung dalam mengharmoniskan regulasi mengenai siber di Indonesia agar dapat selaras, melakukan dan mengadakan kerjasama pada tiap lembaga seperti BSSN atau yang lain yang memiliki kemampuan pada bidang IT dan juga melakukan kerjasama pada industri untuk dapat meningkatkan dan memperkuat pertahanan Indonesia.
3. Kepada pemerintah dan Kementerian Pertahanan Republik Indonesia agar dapat melakukan dan menerapkan pertahanan yang baik yang sesuai pada Undang-Undang No 34 tahun 2004 harus melakukan manajamen yang baik dan harmonis dalam melakukan manajemen pada regulasi pertahanan, sumber daya manusia, anggaran, industri dan teknologi pertahanan, sumber daya informasi, intelijen, potensi pertahanan dan lain-lain agar dapat pertahanan Indonesia menjadi kuat dan siap.
4. Kepada pemerintah dan terutama pada Kementerian Pertahanan Republik Indonesia disarankan untuk melakukan strategi dan langkah untuk dapat membangun sistem siber yang baik.
5. Kepada pemerintah terutama Kementerian Pertahanan Republik Indonesia untuk dapat membeli *renewal signature* agar dapat melakukan *update* pada *principal* nya ini dalam keamanan sistem jaringannya.
6. Untuk Universitas Pertahanan RI sebagai kampus bela negara yang nanti nya dapat membuat kajian, mata kuliah dan penelitian terkait ancaman asimetris dalam hal ini ancaman siber.

B. Rekomendasi Praktis

1. Saran untuk Pemerintah terutama Kementerian Pertahanan memberikan perhatian yang serius dan khusus pada pentingnya sistem siber segera guna mengantisipasi berbagai macam ancaman dan serangan yang mana dapat mengganggu kemanan dan kedaulatan nasional.
2. Strategi pada Pusat Pertahanan Siber dalam upaya membangun sistem siber sudah mempunyai rencana, sistematis dan

terpadu. Akan lebih baik apabila pemerintah melakukan pembangunan pada konsep doktrin pertahanan negara yang komprehensif yang dikarenakan negara memberikan dukungan dan memperdalam kemampuan sumber daya manusia, melakukan mengadopsi dan kajian kembali pada ekosisem pertahanan siber nasional. Membuat kerangka model pertahanan siber yang baik untuk dapat menyempurnakan teori pada pengembangan kebijakan terhadap sulitnya kebijakan untuk dapat menyesuaikan diri namun perkembangan pada teknologi semakin cepat.

3. Saran untuk pemerintah terutama Kementerian Pertahanan Republik Indonesia pada regulasi yang dimiliki yang memiliki keterkaitan dengan ruang siber seharusnya diharmoniskan, selaras dan seimbang agar tidak memperlemah dari sisi kedaulatan dan memberikan hambatan dalam memperkuat sistem pertahanan siber.
4. Saran untuk pemerintah terutama pada Kementerian Pertahanan Republik Indonesia harus dapat memberikan anggaran khusus dalam sistem siber guna memiliki pertahanan siber yang kuat dan siap.
5. Saran untuk pemerintah terutama pada Kementerian Pertahanan Republik Indonesia dan Pusat Pertahanan Siber pada sumber daya manusia untuk dapat memberikan pelatihan dan pendidikan nasional dan internasional, pemberian sertifikasi internasional, dan lain-lain.
6. Saran untuk pemerintah agar dapat menyalaraskan regulasi dan peraturan untuk dapat menerima sumber daya manusia yang non organik dan bukan anggota TNI.
7. Saran untuk pemerintah terutama pada Kementerian Pertahanan Republik Indonesia merekrut mahasiswa di seluruh Indonesia dari berbagai instansi yang memiliki kecerdasan dan kemampuan di bidang IT agar dapat di pekerjakan di Pushansiber dan dijadikan PNS.
8. Saran untuk pemerintah terutama pada Kementerian Pertahanan Republik Indonesia dapat membeli, melakukan pemelihaaran dan melengkapi kekurangan pada bidang *hardware*, *software*, infrstruktur dan *firmware*. Ini dilakukan untuk pertahanan negara menjadi kuat dan keamanan pada jaringan sistem juga tidak mudah rentan dirusak atau di hancurkan oleh para penjahat siber.
9. Saran untuk pemerintah terutama Kementerian Pertahanan Republik Indonesia dan Pusat Pertahanan Siber untuk melakukan identifikasi dan memetakan resiko yang nantinya dapat memberikan gambaran mengenai adanya serangan dan ancaman terhdap sistem pertahanan siber di Indonesia.

10. Saran untuk pemerintah terutama Kementerian Pertahanan Republik Indonesia dan Pusat Pertahanan Siber Melakukan mitigasi risiko dan aset strategis pertahanan yang menjadi incaran dan rentan terhadap adanya serangan dan ancaman yang dihasilkan dari *penetration test*.

Saran untuk pemerintah terutama Kementerian Pertahanan Republik Indonesia dan Pusat Pertahanan Siber Perlu nya membentuk ekosistem pertahanan siber bersama dengan pihak lainnya guna mendapatkan dukungan dari semua pihak yang nantinya dapat melakukan kolaborasi, koordinasi dan kooperasi dengan mudah, efisien dan tepat.

UCAPAN TERIMAKASIH

1. Laksdya TNI Dr. Amarulla Octavian, S.T., M.Sc., DESD selaku Rektor Universitas Pertahanan yang telah memberikan dukungan.
2. Mayjen TNI Dr. Priyanto, S.IP., M.Si (Han) selaku Wakil Dekan Fakultas Strategi Pertahanan.
3. Laksma TNI Dr. Ir. Beni Rudiawan, S.E., M.Si. (Han), M.M selaku Wakil Dekan Fakultas Strategi Pertahanan.
4. Sekretaris Program Studi Peperangan Asimetris, Kolonel Laut (P) Dr. Rudy Sutanto, S.IP., M.M., CIQaR. yang terus memberikan semangat dan bimbingannya kepada saya selama menjalani pendidikan, baik di dalam kampus maupun ketika penelitian.
5. Bapak Laksda TNI Dr. Suhirwan., S.T., M.MT., M. Tr. Opsla., CIQaR., CIQnR., IPU selaku pembimbing satu, yang memberikan arahan dan bimbingan pada penelitian yang saya lakukan.
6. Bapak Kolonel Sus. Dr. Ir. Rudy A.G. Gultom., M.Sc., CEH., CIQaR selaku pembimbing dua, yang memberikan arahan dan bimbingan pada penelitian yang saya lakukan.
7. Bapak Dr. Ir. Agus H.S Reksoprodjo, DIC selaku dosen penguji dan informan, yang telah menjadi penguji dan informan yang memberikan pandangan dan masukkanya terhadap penelitian yang saya kerjakan
8. Bapak Letnan Kolonel Inf. Tiyoga Budi P., M.Si selaku dosen penguji, yang telah meluangkan waktu untuk memberikan arahan, bimbingan terhadap penelitian yang saya kerjakan kepada saya secara khusus.
9. Bapak Mayor Jenderal TNI Tri Yuniarto, S.A.P., M.Si., M.Tr. (Han). selaku Bapak+Papah beserta Mamah, yang selalu memberikan saya semangat, selalu menanyakan "Sekolahnya bagaimana Dek? Jangan pernah takut dan You have to start learning to be brave. Never be afraid of anyone. All humans eat rice. There's nothing to be afraid of." Dan tak luput mendo'akan saya.
10. Bapak Mayor Jenderal TNI Gamal Haryo Putro, S.I.P., M.

Hum., M.S.S. selaku Pakde yang selalu memberikan saya semangat dan memberikan bantuan untuk dapat memiliki kontak para narasumber agar lekas selesai kuliahnya.
11. Bapak Brigadir Jenderal TNI (Purn) Makmur Supriyatno, B.Sc., S.Pd., M.Pd., selaku Dosen di Universitas Pertahan RI dan Informan saya, yang telah membantu, mendukung, dan mendo'akan saya.
12. Mas Andrea Abdul Rachman Azzqy M.Si, M.Si (Han). CCNP., MCTS selaku Bapak Dosen Universitas Budi Luhu dan Abang saya, yang telah membantu, memberikan arahan, mendukung dan mendo'akan saya.
13. Bapak Brigadir Jenderal TNI I Gusti Putu Wirajena, S.T., M.M.S.I selaku Kepala Biro Persidangan, Sistem Informasi, dan Pengawasan Internal di Dewan Ketahanan Nasional, yang menjadi informan dan telah banyak membantu membantu saya dalam menghubungi informan lainnya, mendukung dan serta mendo'akan saya.
14. Bapak David Bezalel Anggo Syah Putra Laoli, S.Kom., M.Si. selaku informan di Pusdatin, yang telah membantu, membimbing dan mendukung saya
15. Bapak Kolonel Chb Damian Adhi Susastyo, S.H. selaku Analis Kebijakan Madya Bid TIK Pusdatin dan informan saya di Pusdatin, yang telah membantu, mendukung, mengarahkan dan mendo'a kan saya.
16. Bapak Kolonel Sus Tri Satya selaku Kepala Bidang Operasi Pushansiber, yang telah membantu, mendukung, mengarahkan dan mendo'a kan saya. I learned a lot from you Sir.
17. 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 Subbidang Keamanan Aplikasi Bidang Penjamin Keamanan Pusat Pertahanan Siber sebagai informan dalam penelitian ini.
18. Bapak Dr. Ir. Achmad Farid W, M. sebagai dosen di perguruan tinggi Universitas Pertahanan Republik Indonesia sekaligus mantan dari Kepala Cyber Defense Pusat Data dan Informasi Kementerian Pertahanan, yang telah menjadi informan pada penelitian ini.
19. Bapak Prof. Dr. Ir. Richardus Eko Indrajit M. Sc., MBA., Mphil. MA sebagai pakar teknologi informatika, yang telah menjadi informan pada penelitian saya.
20. Mas Ardhi Jernih Miko, M. Han, Mbak Elfina, S.I.P., M. Han sebagai staff prodi

peperangan asimetris dan Mami Agnes CHML. Tobing, S.Ikom., M.Han sebagai sekretaris pribadi Kolonel Sus. Dr. Ir. Rudy A.G. Gultom., M.Sc., CEH., CIQaR, yang telah membantu, mendukung dan mendo'a kan saya.

21. Ayang Fazar Sidik, M. Kom sebagai partner saya yang telah membantu, menemani, mendukung dan mendo'a kan saya.
22. Ardhi Fajriansyah, S. Kom sebagai sahabat saya, yang telah membantu saya dalam penelitian ini.
23. Fika Karina, S.I.P sebagai Kakak saya yang selalu memberikan bimbingan, dukungan dan semangat untuk menyelesaikan penelitian ini.
24. Ayah, Ibu, adik, Eyang Uti, nenek, mamah+papah, Mamah Masenah dan Mamah Ning yang selalu memberikan bimbingan dan semangat dalam menghadapi setiap tantangan selama pendidikan.
25. Senior dan Rekan-rekan dari prodi Peperangan Asimetris CO 09, yang selalu memberikan dukungan dan do'a satu sama lainnya.

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