BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

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. 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* (2021) dan *Center for Strategic International Studies* (2021) :

Tabel 1. 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

Tabel 1.1 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 1. 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

Sumber: diolah peneliti 2022

Tabel 1.2 menunjukkan bahwa antara tahun 2017-2021 telah terjadi ancaman serangan siber di Indonesia dengan kategori mengkahawatirkan. Pada tahun 2017, terdapatnya dua rumah sakit yiatu Dharmais dan Harapan Kita yang disinyalir terkena serangan *ransomware* yang berjenis *WannaCry* pada bulan Mei menurut oke*techno* (2017). Kemudian pada tahun 2018 terdapatnya serangan *malware* sebanyak 40% dan adanya kerja sama dengan *HoneyNet* yang mencatat apabila adanya serangan siber menurut CNN Indonesia (2019).

Namun menurut Noor Anjani (2021) 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. Pada tahun 2020 dunia sedang berjuang melawan *covid-19* dan aktor penyerangan telah memanfaatkan kondisi tersebut untuk dapat meraup keuntungan dengan melakukan penyebaran *malware, virus, spam email dan ransomware.* Pasalnya, pada tahun 2021 terjadinya banyak serangan siber yang luar biasa di Indonesia dan dengan kurun waktu tiap tahunnya, terdapat banyak nya serangan siber seperti *malware, phishing, data leak, trojan* yang dapat merugikan, merusak

dan mengganggu Indonesia. Maka ini diperlukan adanya perhatian, kewaspadaan dan antisipasi dengan adanya ancaman siber.

Menurut Erichson Sitohang (2011) Seperti yang dilakukan oleh Hacker dari Malaysia yang telah berhasil meretas situs resmi *website* TNI yang beralamat http://www.tni.mil.id/ pada hari Jum'at 15 Juli 2011. Peretas yang berasal dari Malaysia telah berhasil merubah situs tersebut menjadi tulisan "*This Website Has Been Hacked By m33h00n*" dan meninggalkan jejak dengan kalimat "*Greetings From Malaysia*! By m33h00n & m0rn!ngw00d!". Kemudian adanya peretas kembali yang telah dilakukan oleh dua hacker remaja yang berasal dari kota Batam dan telah ditangkap oleh petugas TNI Angkatan Darat. Mereka telah melakukan peretasan pada situs *website* yang dimiliki oleh pihak TNI AD pada tahun 2021.

Kasus ini awal mulanya melakukan pendeteksian kegiatan pada *Web Defacement* di situs remi TNI AD oleh Patroli Siber Pussansiad pada hari Jum'at 28 Mei 2021. Menurut Ady Purwadi (2021) IP peretas dapat dilacak oleh Pussansiad. Brigjen TNI Iroth Sonny Edhie telah mengemukakan bahwa adanya serangan siber yang didapat seperti virus dan malware sebanyak 200 atau 300 per harinya dan Serangan tersebut masih terbilang umum namun pada ancaman ini memiliki target yang patut di waspadai menurut Rizal (2020).

Menurut Christoper Devon Mahendri (2020) Adanya peretas yang telah menyerang pada situs website dari Sekolah Staf dan Komando Angkatan Darat (Seskoad) yang bersatatus *under maintenance*. Pada situs Pusat Pendidikan Kavaleri TNI AD juga telah di serang oleh para peretas (*hacker).* Tampilan pada situs tersebut telah diganti dengan menggunakan berlatar belakang berwarna hijau dan di susupi kalimat yang berbunyi "*Secret 404 Was HERE*". Telah di temukan jejak nama yang dilakukan oleh para *hacker*, yaitu 404 Cyber Attack dalam Merdeka (2013).

Baru-baru ini telah terjadi penyerangan yang dilakukan oleh peretas atau *Hacker* yang berasal dari negeri tirai bambu, yaitu China. *Hacker* China dikabarkan telah menembus pada 10 jaringan internal kementerian

dan lembaga pemerintah Indonesia, termasuk Badan Intelijen Negara (BIN) yang telah dilaporkan oleh peneliti keamanan internet The Record, Insikt Group dalam CNN Indonesia (2021). Terdapatnya *private ransomware* yang bernama Thanos dengan upaya spionase China dalam menghadapi kondisi di Laut China Selatan. Menurut Anggota Komisi I Dewan Perwakilan Rakyat (DPR) yang berasal dari Fraksi Golkar, yaitu Dave Laksono yang meminta dan mendesak kepada pemerintah agar dapat mempercepat pada proses pembahasan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) dengan DPR dalam CNN Indonesia (2021). Dengan terbentuknya undang-undang tersebut agar lebih berkualitas, tidak mudah diretas para *hacker* guna melindungi dan menjaga data pribadi dan dokumen rahasia yang dimiliki pemerintah Indonesia.

Dari penjelasan diatas mengenai bentuk serangan siber yang di alami oleh Indonesia sendiri yang dikarenakan belum maksimal dan optimalnya dalam membangun sistem siber. Jenis-jenis *malware* yang biasanya digunakan para peretas sepertiL virs*, worm, trojan horse, spyware* dan *executable bot*. Menurut Aidil sumber daya manusia di Indonesia pada bidang siber yang memiliki kemampuan dalam menangkal dan mengatasi serangan siber masih belum optimal dan masih pada tahap pengembangan, yang kemudian ditambah dengan belum cukupnya jumlah anggota yang dimiliki dalam Universitas Teknologi Yogyakarta (2018). Ini menjadi catatan bagi Pusat Pertahanan Siber di Kementerian Pertahanan agar dapat meningkatkan perlindungan dan menjaga pertahanan Indonesia dari serangan siber.

Menurut Noor Anjani (2021) Di Indonesia telah memiliki dasar hukum yang mana mengatur pada keamanan siber adalah UU Informasi dan Transaksi Elektronik (ITE) No 11 Tahun 2008 dan adanya revisi UU ITE No 19 Tahun 2016 yang menjelaskan adanya beberapa pelanggaran seperti pelanggaran pada perlindungan data, pendistribuasian konten yang ilegal, terdapatnya akses yang tidak memiliki izin pada sistem komputer guna mendapatkan informasi dan dapat memberikan perlindungan hukum pada transkasi elektronik dan konten sistem elektronik.

Namun pada UU ITE No 19 Tahun 2016, pemerintah mengeluarkan Peraturan Pemerintah (PP) No 71 Tahun 2019 mengenai Penyelenggaraan Sistem dan Transaksi Elektronik yang mana pada peraturan tersebut memiliki pembaharuan mengenai keamanan siber pada sistem dan transaksi elektronik. Kemanan dunia siber sangat diperlukan guna menjaga integritas, menjaga data dan ketersediaan informasi digital yang dimiliki oleh suatu negara. Maka dari itu ancaman serangan siber menjadi bentuk perhatian dan kerawanan yang besar bagi kita semua.

Pertahanan nasional dihadapkan dengan situasi berkembangnya teknologi 4.0, maka dari itu perlu adanya pembangunan, pengembangan dan peningkatkan pertahanan nasional untuk dapat menangkal adanya ancaman militer dan nirmiliter yang dapat mengganggu pertahanan nasional. Globalisasi telah terlibat secara langsung ataupun tidak langsung kepada sektor teknologi dan informasi, ideologi, ekoenomi, sehingga karakteristik Indonesia telah mengalami perubahan dengan adanya ancaman.

Menurut Makmur Supriyatno (2014), mengatakan mengenai ilmu pertahanan menjadi suatu ilmu yang berasal dari strategi, Ilmu militer dan ilmu &ilmu seni perang. Kita semua juga harus mempelajari dan mengetahui bagaimana untuk dapat merencanakan dan mempersiapkan seluruh sumber daya kekuatan militer yang menitik balikan kepada strategi dan taktik untuk dapat mencapai keunggulan dan kemenangan perang. Menurut Libick dalam buku Riekhoff (2000) pada artikelnya mengenai

"*What is information warfare*?" telah melihat masyarakat yang modern, sudah masuk kedalam kelompok militer yang memiliki ketergantungan pada sistem informasi. Ini telah menghasilkan suatu dampak pada perangan informasi. Kemudian Libick telah mengelompokkan perang informasi menjadi 7 bagian, yaitu:

1) Komando dan Kendali (*Command and Control Warfare*)
2) Perang berbasis Intelijen (*Intelligent based Warfare)*
3) Perang Elektronik (*Electronic Warfare*)
4) Perang Psikologi (*Psychology Warfare*)
5) *Hacker Warfare*
6) Perang Informasi Ekonomi (*Economic Information Warfare*)
7) *Cyber Warfre*

Pada perang hibrida telah menggabungkan antara unsur militer dengan nirmiliter Tempo (2021). Pertahanan negara sangat diperlukan sebagai bentuk dari usaha negara guna menjaga dan melindungi bangsa Indonesia dari adanya ancaman dalam Undang-Undang No 3 Tahun 2002 (2002). Sistem pertahanan di Indonesia bersifat semesta, yaitu suatu strategi yang melibatkan setiap warga negara, wilayah dan sumber daya nasional agar di persiapkan secara terpadu dan terarah untuk dapat menuju kedaulatan negara, keutuhan wilayah dan keselamatan bagi bangsa dan negara dari segala bentuk ancaman menurut Sahat M Sinaga (2012).

Yang telah disampakan oleh Makmur Supriyatno (2014) mengenai ilmu pertahanan bahwa pertahanan negara memiliki fungsi dan tugas yang telah di amanatkan pada Undang-undang Republik Indonesia Nomor 3 Tahun 2002 ayat 1 (2002), yaitu untuk dapat mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia dari adanya ancaman dan gangguan terhadap keutuhan bangsa dan negara. Menurut Makmur Supriyatno (2014) Pertahanan negara menjadikan sebagai upaya untuk dapat menuju kedaulatan, mempertahankan keutuhan wilayah Negara Kesatuan Republik Indonesia dan keselamatan bangsa dan negara terhdap adanya ancaman militer dan nirmiliter.

Pengelolaan pertahanan dapat dilakukan melalui sistem pertahanan militer dan nirmiliter yang mengerahkan unsur kekuatan mliter yang disesuaikan melalui kebijakan dan keputusan dari politik negara. Bentuk ancaman siber dapat berasal dari kelompok kejahatan yang terorganisir, permusuhan, kekecewaan, internal dan eksternal, persaingan dan memiliki konflik teknologi. Menurut Ratno Dwi Putra, Supartono, Deni D.A.R. (2018) kondisi tersebut di perkuat dengan keahlian yang dapat mengganggu, merusak dan bahkan dapat mengancam kerahasiaan (*confidentiality*), integritas (*integrity) dan ketersedian (availability*) dari sistem informasi yang dimiliki. Ancaman siber tersebut dapat merusak infrastruktur kritis pada sektor militer.

Menurut Handrini Ardiyanti (2016) terdapatnya beberapa masalah dalam pembangunan keamanan *cyber* di suatu negara seperti terdapatnya kurang penanganan dalam penyerangan siber, kurangnya pemahaman pada pelenyeranggaran disuatu negara mengenai keamanan pada dunia siber, perlunya membentuk tata kelola ada kelembagaan keamanan siber nasional, kurangnya edukasi menegenai kesadaran terhadap adanya serangan atau ancaman pada dunia siber yang dapat merusak dan melumpuhkan negara, kurangnya infrastruktur pada pembangunan sistem siber, belum optimalnya pada industri guna memperoduksi atau mengembangkan produk pada perangkat keras, terbatasnya sumber daya manusia yang memiliki kemampuan pada bidang siber dan anggaran yang dimiliki tidak cukup.

Menurut Rudy Gultom (2018), 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)*

Pada ilmu pertahanan yang telah dijelaskan oleh Makmur Supriyatno (2018), yaitu adanya manajemen sumber daya manusia pertahanan, manajemen industri dan teknologi pertahanan, manajemen sumber daya informasi, intelijen dan pengetahuan pertahanan, *Stakeholder* pertahanan dan manajemen keungan pertahanan dan sumber daya anggaran. Dari penjelasan diatas telah menunjukkan adanya keterkaitan antara teori SWNSF dan teori ilmu pertahanan satu sama lain yang memiliki usaha dalam mempertahankan negara dan membangun sistem pertahanan siber Indonesia.

Kemudian strategi wilayah pada pertahanan negara Indonesia mengacu pada pertahanan negara yang memiliki fungsi untuk dapat mewujudkan dan mempertahankan seluruh Negara Kesatuan Republik Indonesia sebagai satu kesatuan pertahanan. Dari strategi inilah yang menjadi proses penentu pada rencana bagi para pemimpin yang memiliki fokus pada tujuan jangka panang yang mana dibarengi dengan penyusunan suatu upaya atau cara agar bagaimana strategi dari Pushansiber membangun sistem siber dalam menghadapi ancaman siber yang menajdi tujuan yang dicapai.

Indonesia berusaha untuk membangun dan meningkatkan sistem pertahanan siber melalui penguatan teknologi dan informasi pada sistem siber. Ancaman siber dapat dilakukan ketika suatu negara memiliki kelemahan pada teknologi dan informasi yang nantinya akan dapat mengancam kedaulatan dan keutuhan negara Indonesia. Pelbagai ancaman serangan siber yang lama telah dimodivikasi dalam penyerangan siber yang terbaru. Sistem siber seharusnya menjadikan sebuah strategi dalam menjaga dan melindungi pertahanan negara yang masuk dalam keamanan nasional dengan mengembangkan konsep SWNSF.

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**"

Dengan penelitian ini, diharapkan penulis dapat melihat "bagaimana strategi pertahanan siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia". Disisilain, diharapkan penelitian ini dapat menjadi sebagai bahan pertimbanagan dan saran dalam pengambilan keputusan kedepan bagi Pemerintah Indonesia dan TNI dalam meningkatkan sistem siber secara menyeluruh dalam mencegah ancaman siber guna meningkatkan pertahanan negara Indonesia.

1.2 Fokus dan Sub Fokus Penelitian

Fokus penelitian dalam tesis ini adalah permasalahan terkait dengan strategi pertahanan siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan. Pemilihan fokus tersebut dilakukan untuk dapat membatasi permasalahan yang diangkat oleh peneliti. Adapun sub fokus yang peneliti ambil, seperti:

a. Faktor-faktor kendala pendukung dalam membangun sistem siber guna menghadapi ancaman siber
b. Strategi pertahanan siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia
c.

1.3 Rumusan Masalah

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?

1.4 Tujuan Penelitian

Dalam pembuatan penelitian ini, penulis memiliki beberapa tujuan hendak di peroleh sebagai berikut:

a. Menganalisis faktor-faktor kendala dalam membangun sistem siber guna menghadapi ancaman siber
b. Menganalisis strategi pertahanan siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia guna menghadapi ancaman siber

1.5 Manfaat Penelitian

Manfaat dari penelitian ini diharapkan mampu meberikan informasi mengenai strategi pertahanan siber Indonesia di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia guna menghadapi ancaman siber yang ditinjau dari perangkat dan teknologi, sumber daya manusia, perencanaan strategi, ancaman, arsitektur dan *budgeting*. Penilitian ini menjadikan sangat penting untuk menganalisis bagaimana kesiapan dari pertahanan Indonesia dalam membangun sistem siber dalam menghadapi ancaman siber.

1.6 Manfaat Teoritis

Secara teoritis, penelitian ini diharapkan dapat memberikan pengembanagan pada ilmu pengetahuan, adanya kontribusi untuk memperkaya dalam kajian bidang pertahanan nasional khususnya peperangan asimetris mengenai adanya ancaman siber di Indonesia yang harus diperhatikan. Ancaman siber termasuk salah satu kajian yang penting dalam peperangan asimetris. Penelitian ini mempunyai manfaat teoritis bagi beberapa pihak, yaitu:

a. Kelompok Akademisi: Penelitian ini bertujuan untuk memberikan pentingnya pemahaman mengenai ancmaan siber yang terjadi di Indonesia.
b. Peneliti lain: Penelitian ini dapat memberikan manfat dan gambaran bagi peneliti selanjutnya yang ingin meneliti pada bidang siber.

1.7 Manfaat Praktis

Penelitian ini dapat memberikan manfaat sebagai berikut:

a. Bagi kementerian/lembaga terkait: sebagai masukan mengenai strategi yang dapat dilakukan oleh Indonesia terutama Kementerian Pertahanan dalam rangka membangun sistem siber khususnya sebagai ancaman siber dan segala bentuk dukungan terhadap membangun dam meningkatkan kemampuan pada sistem siber.
b. Bagi Pemerintah Indonesia: penelitian ini bertujuan untuk memberikan masukan mengenai pentingnya kerjasama yang dijalin antar institusi, baik dalam lingkup global, regional maupun lokal agar dapat mengintegrasikan terhadap teknologi informasi atas adanya ancaman siber yang dapat mengganggu sistem pertahanan nasional yang nanti dan dapat memaksimalkan untuk dapat menangkal, mencegah dan memperkuat siber pertahanan negara Indonesia.
c. Bagi penulis, diharapkan mendapatkan ilmu dalam pemahaman dan pengalaman langsung mengenai hal-hal yang berhubungan dengan kedaulatan pertahanan negara dan dapat memberikan masukan terhadap ilmiah dari berbagai kajian siber di Universitas Pertahanan.