SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 1
JULI 2025

STRATEGI PERTAHANAN SIBER KOOPSUDNAS DALAM RANGKA MENDUKUNG PERTAHANAN UDARA NASIONAL

Putu Sucahyadi
putu@gmail.com

[1]Universitas Pertahanan Republik Indonesia,

Abstract. *The development of information technology has a significant impact on national air defense, particularly in the face of increasingly complex cyber threats. This study analyzes cyber threats to air defense and formulates a strategy for improving the cyber defense system at Koopsudnas. This research method uses a qualitative approach to understand the phenomenon in depth, with a focus on interpretation and description. The methods used include expert interviews and a SWOT analysis. The results indicate that Koopsudnas' cyber defense is not yet optimal, with limitations in regulations, human resources, and technology. Threats such as defacement, data leaks, and exploitation of security gaps require a rapid response. The proposed strategy includes improving regulations, developing human resources, and modernizing technology. Implementing this strategy is expected to strengthen national cyber resilience. An effective strategy for improving cyber defense at Koopsudnas involves strengthening regulations, improving the quality of personnel, and investing in advanced technology. Strong and structured regulations must be accompanied by better inter-agency coordination. Furthermore, increasing the number and quality of cybersecurity personnel must be supported by ongoing training and certification programs. In the technological field, the adoption of intrusion detection systems, firewalls, data encryption, and the use of artificial intelligence (AI) can improve the effectiveness of cyber defense.*

.

Keywords*: cyber defense, Koopsudnas, national air defense, cyber threats, defense strategy*.

Abstrak. Perkembangan teknologi informasi berdampak signifikan pada pertahanan udara nasional, terutama menghadapi ancaman siber yang semakin kompleks. Penelitian ini menganalisis ancaman siber terhadap pertahanan udara dan merumuskan strategi peningkatan sistem pertahanan siber di Koopsudnas. Metode penelitian ini menggunakan pendekatan kualitatif untuk memahami fenomena secara mendalam, dengan fokus pada interpretasi dan deskripsi. Metode yang digunakan meliputi wawancara ahli dan analisis SWOT. Hasil penelitian menunjukkan bahwa pertahanan siber Koopsudnas belum optimal, dengan keterbatasan regulasi, SDM, dan teknologi. Ancaman seperti *defacement*, kebocoran data, dan eksploitasi celah keamanan memerlukan respons cepat. Strategi yang diusulkan mencakup peningkatan regulasi, pengembangan SDM, dan modernisasi teknologi. Implementasi strategi ini diharapkan memperkuat ketahanan siber nasional. Strategi yang efektif untuk meningkatkan pertahanan siber di Koopsudnas melibatkan penguatan regulasi, peningkatan kualitas personel, dan investasi dalam teknologi canggih. Regulasi yang kuat dan terstruktur harus disertai dengan koordinasi antar lembaga yang lebih baik. Di sisi lain, peningkatan jumlah dan kualitas personel keamanan siber harus didukung dengan program pelatihan dan sertifikasi yang berkelanjutan. Di bidang teknologi, adopsi sistem deteksi intrusi, firewall, enkripsi data, dan pemanfaatan kecerdasan buatan (AI) dapat meningkatkan efektivitas pertahanan siber

Kata kunci: pertahanan siber, Koopsudnas, pertahanan udara nasional, ancaman siber, strategi pertahanan.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 1
JULI 2025

1. LATAR BELAKANG

Sejak awal abad ke-21, perkembangan teknologi informasi telah membawa perubahan signifikan, khususnya dalam pertahanan Indonesia. Teknologi informasi dan komunikasi menjadi elemen kunci dalam strategi pertahanan nasional di era digital, termasuk dalam pengembangan sistem pertahanan siber untuk melindungi infrastruktur vital dari serangan siber (Denning, 2014). Selain itu, teknologi juga digunakan dalam pengembangan sistem pertahanan udara, laut, dan darat untuk menghadapi ancaman eksternal (Krisnata dkk, 2022). Dengan meningkatnya penetrasi internet di Indonesia, aktivitas siber juga meningkat, yang memunculkan tantangan baru dalam bentuk ancaman siber yang lebih canggih dan kompleks, terutama yang berkaitan dengan pertahanan udara.

Penelitian ini berfokus pada strategi pertahanan siber dalam mendukung pertahanan udara nasional. Subfokus penelitian mencakup dua hal, yaitu pertama, analisis permasalahan dan kendala pertahanan siber dalam sistem pertahanan udara nasional di Koopsudnas; dan kedua, perumusan strategi yang efektif untuk meningkatkan kemampuan pertahanan siber Koopsudnas dalam aspek regulasi, SDM, dan teknologi.

2. TINJAUAN PUSTAKA

Landasan teori dalam penelitian ini merujuk pada pernyataan terstruktur yang membantu menganalisis dan menggambarkan fenomena, serta merumuskan hipotesis dan meramalkan hasil (Moeloeng, 2004). *Grand theory* yang digunakan mencakup Teori Pertahanan Negara dan Teori Kekuatan. Teori Pertahanan Negara menjelaskan strategi negara dalam menjaga kedaulatan dan menghadapi ancaman, seperti yang diuraikan oleh Huntington mengenai benturan peradaban serta Liddell Hart tentang pendekatan tidak langsung dalam strategi militer. Hans Morgenthau menyoroti pentingnya kekuasaan dan kebijakan realistis dalam pertahanan. Teori Kekuatan, seperti yang dijelaskan oleh Kenneth Waltz, menekankan distribusi kekuatan dalam sistem internasional, sedangkan Keohane dan Nye membahas interdependensi antarnegara. *Middle theory*, seperti Teori Air Power oleh Douhet, menggarisbawahi pentingnya dominasi udara, dan Teori Penangkalan oleh Schelling serta Jervis menekankan pentingnya ancaman dalam mencegah serangan. Arthur Lykke juga menyusun teori strategi yang menghubungkan alat, cara, dan tujuan dalam pertahanan siber. *Micro theory* mencakup Teori Pertahanan Siber, dengan pendekatan berlapis-lapis dan serangan proaktif (Clarke & Knake), serta Teori Teknologi Informasi yang menguraikan penerimaan dan inovasi teknologi dalam konteks pertahanan siber.

3. METODE PENELITIAN

Metode penelitian ini menggunakan pendekatan kualitatif untuk memahami fenomena secara mendalam, dengan fokus pada interpretasi dan deskripsi daripada pengukuran kuantitatif. Teknik pengumpulan data meliputi wawancara mendalam, observasi, dan analisis dokumen, yang memberikan wawasan tentang interaksi antaraktor dalam manajemen ruang udara nasional. Desain penelitian yang digunakan adalah deskriptif kualitatif dengan analisis data menggunakan Teknik Miles dan Huberman, yang mencakup reduksi data, penyajian data, dan penarikan kesimpulan untuk mengidentifikasi pola, tema, dan hubungan antarvariabel yang

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
JULI 2025

kompleks. Hal ini memungkinkan peneliti mengelola data kualitatif secara sistematis dan menghasilkan pemahaman yang mendalam tentang implementasi pertahanan siber di Koopsudnas.

Penelitian ini dilakukan di Koopsudnas, Kosek IKN, dan Satsiber Dispamsanau selama periode 19 hingga 21 Juni 2024. Subjek penelitian mencakup personel dari berbagai instansi yang terlibat dalam pertahanan udara, sedangkan objek penelitian berfokus pada optimalisasi pertahanan siber untuk mendukung pertahanan udara nasional. Teknik pengumpulan data mencakup studi literatur, dokumentasi, dan wawancara, sementara keabsahan data diverifikasi melalui triangulasi dan diskusi. Analisis data dilakukan dengan model interaktif yang melibatkan tiga tahap utama: kondensasi data, penyajian data, dan penarikan kesimpulan.

4. HASIL DAN PEMBAHASAN

Hasil wawancara di Koopsudnas dan TNI AU menunjukkan bahwa pertahanan siber saat ini didukung oleh regulasi seperti Perkasau Nomor 19 Tahun 2020 dan Undang-Undang No. 1 Tahun 2024, serta oleh SDM yang terlatih dan tersertifikasi. Namun, jumlah SDM masih terbatas, dan teknologi yang digunakan, meskipun mencakup perangkat seperti firewall dan IDS/IPS, belum sepenuhnya memenuhi kebutuhan keamanan siber yang optimal. Ancaman yang dihadapi, termasuk web defacement, kebocoran data, dan serangan terhadap sistem komando dan kendali, menunjukkan adanya kerentanan dalam infrastruktur pertahanan udara. Tantangan utama meliputi peningkatan jumlah dan kemampuan SDM, pembaruan regulasi, dan pengembangan teknologi yang lebih canggih seperti SIEM dan AI untuk meningkatkan deteksi dan respons terhadap ancaman siber.

Strategi peningkatan pertahanan siber di Koopsudnas mencakup penguatan regulasi, pengembangan SDM, dan modernisasi teknologi. Dari sisi regulasi, diperlukan kebijakan yang lebih komprehensif, audit reguler, dan koordinasi antara lembaga terkait. Dari sisi SDM, peningkatan pelatihan, sertifikasi, dan rekrutmen spesialis keamanan siber menjadi prioritas, sementara dari aspek teknologi, Koopsudnas membutuhkan integrasi sistem keamanan yang lebih canggih, seperti SIEM dan IDS/IPS, serta pembangunan laboratorium siber untuk pengujian dan simulasi serangan. Langkah-langkah ini diharapkan dapat meningkatkan kemampuan Koopsudnas dalam melindungi infrastruktur dan informasi vital dari ancaman siber yang terus berkembang.

Analisis wawancara tentang kemampuan pertahanan siber Koopsudnas mengungkapkan beberapa tantangan utama, termasuk keterbatasan jumlah personel terlatih dan belum meratanya instalasi teknologi keamanan siber. Meskipun regulasi yang ada, seperti Perkasau Nomor 19 Tahun 2020, sudah memberikan kerangka dasar, masih diperlukan pengembangan lebih lanjut untuk mencapai efektivitas maksimal. Ancaman siber yang dihadapi Koopsudnas mencakup serangan terhadap sistem komando, kendali, dan radar, serta kebocoran data sensitif. Tantangan lain meliputi kekurangan SDM berkualitas, kurangnya koordinasi antara lembaga, dan keterbatasan anggaran untuk teknologi baru.

Strategi peningkatan pertahanan siber di Koopsudnas berfokus pada penguatan regulasi, peningkatan SDM melalui pelatihan berkelanjutan, dan modernisasi teknologi dengan alat seperti SIEM dan IDS/IPS. Kolaborasi antara sektor pemerintah, swasta, dan TNI AU menjadi sangat penting untuk memperkuat pertahanan siber secara keseluruhan. Selain itu, pendidikan dan pelatihan berkelanjutan, serta peningkatan kesadaran keamanan siber, menjadi prioritas untuk menghadapi ancaman yang semakin kompleks di masa depan.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
JULI 2025

Hasil wawancara mengungkapkan bahwa meskipun Koopsudnas telah memiliki dasar regulasi yang mendukung pertahanan siber, seperti Perkasau Nomor 19 Tahun 2020 dan Keputusan Kasau Nomor Kep/424/XI/2022, implementasinya masih perlu pengembangan lebih lanjut. Mengacu pada teori strategi Carl Von Clausewitz, strategi yang efektif harus dirancang berdasarkan realitas di medan perang, dan dalam konteks ini, regulasi yang ada perlu ditingkatkan agar lebih responsif terhadap ancaman yang terus berkembang. Arthur F. Lykke menekankan pentingnya keseimbangan antara tujuan, cara, dan sumber daya. Saat ini, keterbatasan jumlah personel yang terlatih mengindikasikan ketidakseimbangan antara cara dan sumber daya, sehingga menghambat pencapaian tujuan pertahanan siber optimal. Hal ini sejalan dengan penelitian Nugroho dan Resnawaty (2023) yang menunjukkan kurangnya kesiapan perlawanan elektronika di TNI AU karena keterbatasan personel dan teknologi.

Ancaman siber terhadap sistem pertahanan udara nasional di Koopsudnas mencakup berbagai bentuk serangan, seperti *malware*, *ransomware*, *Advanced Persistent Threats* (APT), serangan *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS), *phishing*, serta eksploitasi kerentanan perangkat lunak. Serangan *malware* dan *ransomware* dapat melumpuhkan infrastruktur kritis dengan mencuri data atau mengunci akses hingga tebusan dibayar, sementara APT yang sering didukung negara bertujuan untuk pencurian data sensitif dan pemantauan jangka panjang. Serangan DoS/DDoS dapat mengganggu komunikasi dan sistem radar, menghambat respons pertahanan udara. Selain itu, *phishing* dan rekayasa sosial menargetkan personel militer untuk mendapatkan akses tidak sah, dan kerentanan perangkat lunak yang tidak diperbarui menjadi celah bagi penyerang. Contoh nyata seperti serangan ransomware terhadap Pusat Data Nasional dan serangan Stuxnet menyoroti betapa rentannya infrastruktur pertahanan terhadap serangan siber.

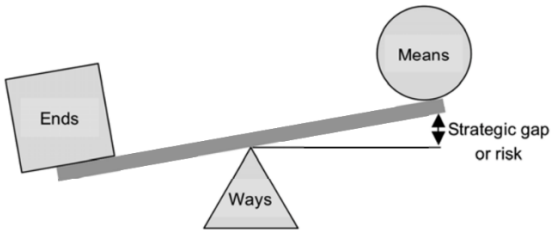
Serangan siber terhadap sistem pertahanan udara nasional di Koopsudnas memiliki dampak signifikan dari berbagai aspek, termasuk operasional, ekonomi, sosial, dan teknologi. Dampak operasional mencakup gangguan pada operasi pertahanan, pencurian data, serta pelumpuhan infrastruktur melalui serangan malware dan ransomware. Dari sisi ekonomi, biaya pemulihan sistem yang terinfeksi dan kerusakan teknologi dapat mencapai angka signifikan, mempengaruhi stabilitas ekonomi nasional, terutama sektor penerbangan. Secara sosial, serangan ini dapat menyebabkan ketidakpercayaan dan kecemasan publik mengenai kemampuan pertahanan negara, sementara secara teknologi, serangan dapat memaksa TNI mempercepat pembaruan teknologi dan memperkuat infrastruktur keamanan sibernya. Dengan dampak yang begitu luas, Koopsudnas memerlukan strategi pertahanan siber yang komprehensif untuk melindungi infrastruktur vital dan menjaga keamanan nasional.

Tantangan utama dalam meningkatkan pertahanan siber di Koopsudnas meliputi keterbatasan personel, regulasi yang belum komprehensif, serta integrasi teknologi yang belum optimal. Keterbatasan personel menghambat efektivitas strategi siber, karena sumber daya manusia yang terbatas tidak seimbang dengan kebutuhan operasional. Teori strategi dari Clausewitz dan Lykke menunjukkan bahwa keseimbangan antara tujuan, cara, dan alat sangat penting untuk mencapai hasil yang diinginkan, sehingga peningkatan kualitas dan kuantitas personel serta penguatan regulasi menjadi sangat krusial. Selain itu, regulasi yang belum mendukung sepenuhnya menyebabkan pelaksanaan kebijakan siber menjadi tidak terarah, sementara integrasi teknologi yang belum maksimal memperlambat kemampuan pertahanan siber dalam merespons ancaman modern.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
JULI 2025

Selain itu, hambatan dalam implementasi strategi pertahanan siber di Koopsudnas mencakup keterbatasan anggaran, kurangnya koordinasi antar lembaga, dan regulasi yang belum memadai. Keterbatasan anggaran menghambat pengadaan teknologi dan pelatihan personel yang diperlukan, sementara koordinasi yang buruk antara lembaga seperti TNI AU dan pemerintah mengakibatkan kebijakan yang tumpang tindih. Teori Morgenthau menekankan pentingnya keamanan nasional sebagai prioritas utama, yang mengharuskan pengelolaan anggaran dan sumber daya secara efektif. Untuk menghadapi hambatan ini, Koopsudnas harus meningkatkan kolaborasi antar lembaga dan mengembangkan regulasi yang lebih kuat, seperti yang disarankan oleh penelitian Wijaya dkk, serta mengikuti prinsip keseimbangan strategi dari Clausewitz dan Lykke.

Strategi pertahanan siber di Koopsudnas didasarkan pada pendekatan komprehensif teori *Ends, Ways, Means, and Risk* (EWMR), yang membantu merumuskan langkah-langkah strategis secara sistematis dan terstruktur. *Ends* mengacu pada tujuan utama seperti peningkatan ketahanan siber dan perlindungan sistem pertahanan udara nasional dari ancaman siber. *Ways* mencakup metode yang digunakan, seperti penyusunan regulasi, peningkatan kapasitas SDM, dan adopsi teknologi canggih. *Means* merujuk pada sumber daya yang diperlukan, seperti anggaran, teknologi, dan personel. Sementara *Risk* melibatkan identifikasi risiko, termasuk keterbatasan anggaran dan tantangan teknologi, yang harus dimitigasi untuk memastikan implementasi strategi berjalan optimal. Pendekatan ini bertujuan memberikan solusi holistik untuk memperkuat pertahanan siber Koopsudnas.



Gambar 1
Ends, Ways, Means* dan *Risk

Tabel 1
Ends, Ways, Means* dan *Risk

Kategori	Deskripsi
***Ends* (Tujuan)**	- Meningkatkan ketahanan siber Koopsudnas. - Melindungi sistem pertahanan udara nasional dari ancaman siber. - Meningkatkan respons terhadap insiden siber.
***Ways* (Konsep)**	- Pengembangan regulasi yang kuat dan komprehensif. - Pelatihan dan pengembangan SDM yang berkelanjutan. - Implementasi teknologi canggih seperti IDS/IPS, firewall, SIEM, dan enkripsi. - Koordinasi antar lembaga untuk berbagi informasi dan pelatihan bersama.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
JULI 2025

Kategori	Deskripsi
	- Pembentukan tim tanggap insiden siber. - Pembangunan SOC dan NOC. - Penggunaan teknologi open source dan kecerdasan buatan. - Pembaruan dan pemeliharaan sistem secara rutin.
***Means* (Sumber Daya)**	- Anggaran yang cukup untuk pengadaan teknologi canggih dan pelatihan. - Rekrutmen spesialis keamanan siber. - Fasilitas pendukung seperti lab siber. - Kolaborasi dengan institusi pendidikan dan perusahaan teknologi. - Dukungan dari lembaga pemerintah lainnya.
***Risk* (Risiko)**	- Keterbatasan anggaran yang dapat menghambat pengadaan dan pelatihan. - Serangan siber yang semakin canggih dan sulit dideteksi. - Kurangnya kesadaran dan kesiapan personel. - Koordinasi antar lembaga yang tidak optimal.

Tujuan utama strategi pertahanan siber di Koopsudnas adalah untuk meningkatkan ketahanan dan keamanan sistem pertahanan udara nasional dari ancaman siber yang semakin kompleks. Hal ini sejalan dengan teori Samuel P. Huntington yang menekankan pentingnya pertahanan terhadap ancaman non-konvensional seperti serangan siber yang dapat merusak stabilitas nasional. Selain itu, strategi ini bertujuan membangun kemampuan deteksi, respons, dan pemulihan yang efektif terhadap insiden siber, dengan dukungan regulasi dan prosedur terstruktur, sebagaimana dijelaskan oleh teori strategi Clausewitz dan Lykke. Pendidikan dan pelatihan berkelanjutan juga menjadi prioritas untuk meningkatkan kesiapan personel menghadapi ancaman siber, didukung oleh model penerimaan teknologi Fred Davis. Koordinasi dan kolaborasi dengan berbagai pemangku kepentingan, baik nasional maupun internasional, diperkuat untuk menghadapi ancaman siber secara kolektif, sesuai dengan teori kekuatan Kenneth N. Waltz dan teori interdependensi Robert O. Keohane dan Joseph S. Nye Jr.

Strategi pertahanan siber di Koopsudnas dirancang dengan pendekatan yang komprehensif melalui teori EWMR yang mencakup aspek regulasi, sumber daya manusia (SDM), dan teknologi. Dari aspek regulasi, strategi ini menekankan pentingnya regulasi yang kuat dan komprehensif untuk mendukung pertahanan siber. Penyusunan kebijakan keamanan siber mencakup beberapa aspek penting, seperti enkripsi data, manajemen akses, dan pemantauan jaringan. Kebijakan enkripsi harus melindungi data sensitif baik saat disimpan maupun ditransmisikan menggunakan metode seperti AES-256. Manajemen akses perlu diatur dengan sistem otentikasi ganda (MFA) dan sistem manajemen identitas untuk mencegah akses yang tidak sah. Selain itu, pemantauan jaringan secara real-time dengan sistem seperti IDS/IPS dan SIEM sangat penting untuk mendeteksi ancaman siber secara proaktif.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
JULI 2025

Koordinasi antar lembaga dalam keamanan siber harus ditingkatkan melalui berbagi informasi dan pelatihan bersama. Sistem berbagi informasi yang aman, seperti Threat Intelligence Platform (TIP), dapat mempercepat respons terhadap ancaman siber. Selain itu, pelatihan dan simulasi serangan siber antar lembaga, seperti yang melibatkan TNI dan BSSN, akan meningkatkan kesiapan kolektif dan memperkuat kerja sama dalam menghadapi ancaman siber.

Audit reguler dan kepatuhan terhadap standar keamanan siber sangat penting untuk mengidentifikasi kelemahan dan mengurangi risiko. Audit berkala memastikan bahwa kebijakan keamanan siber seperti enkripsi dan manajemen akses diimplementasikan dengan benar. Penegakan kepatuhan harus disertai dengan sanksi bagi yang melanggar dan insentif bagi yang mematuhi regulasi. Sistem pelaporan insiden keamanan siber juga harus diimplementasikan untuk meningkatkan respons terhadap ancaman.

Pembangunan *Security Operations Center* (SOC) di Koopsudnas akan menjadi pusat pengawasan keamanan siber. SOC akan memantau, mendeteksi, dan merespons ancaman siber secara real-time, serta memastikan bahwa kebijakan dan protokol keamanan siber dipatuhi. SOC terdiri dari tim-tim khusus yang bertanggung jawab untuk deteksi dan analisis ancaman, serta respons insiden, didukung oleh teknologi canggih seperti SIEM, IDS, dan IPS.

SOC di Koopsudnas akan dilengkapi dengan berbagai teknologi untuk memantau dan melindungi jaringan. SIEM berfungsi sebagai alat utama untuk mengumpulkan dan menganalisis data dari berbagai sumber, sementara IDS/IPS digunakan untuk mendeteksi dan mencegah ancaman. Teknologi tambahan seperti firewall dan VPN akan digunakan untuk menjaga keamanan jaringan, serta alat forensik digital untuk investigasi pasca-insiden.

Selain SOC, diperlukan juga pembangunan *Network Operations Center* (NOC) untuk jajaran di bawah Koopsudnas seperti Koopsud, Kosek, dan Lanud. NOC akan berfungsi sebagai pusat operasi jaringan untuk mendukung upaya pertahanan siber secara lebih luas. NOC akan memantau jaringan dan memastikan kelancaran operasional serta keamanan jaringan di setiap wilayah komando.

Penelitian menunjukkan bahwa tanpa regulasi yang terstruktur dan koordinasi yang baik, upaya untuk memperkuat pertahanan siber akan sulit terwujud, sehingga Koopsudnas perlu memastikan pelaksanaan regulasi yang tepat untuk meningkatkan keamanan siber secara menyeluruh.

Sumber daya manusia yang kompeten dalam keamanan siber sangat penting untuk memastikan sistem pertahanan yang tangguh. Pelatihan berkelanjutan dan sertifikasi untuk personel yang terlibat menjadi kebutuhan yang mendesak. Program pelatihan teknis harus mencakup cara mendeteksi dan merespons serangan siber, serta pengetahuan tentang regulasi dan kebijakan terkait. Kerja sama dengan institusi pendidikan dan pelatihan yang memiliki keahlian dalam pertahanan siber juga diperlukan untuk mengembangkan kurikulum yang sesuai dengan kebutuhan pertahanan nasional.

Dalam kerangka teori strategi Carl Von Clausewitz dan Arthur F. Lykke, sumber daya manusia yang terlatih dianggap sebagai elemen esensial untuk mencapai tujuan strategis pertahanan siber. Penelitian menunjukkan bahwa tanpa SDM yang memadai, meskipun teknologi canggih tersedia, kemampuan untuk mengoperasikan dan mempertahankannya akan terbatas. Oleh karena itu, peningkatan kapasitas dan kapabilitas SDM dalam pertahanan siber menjadi kebutuhan yang tidak bisa diabaikan, terutama untuk menjaga kesiapan menghadapi ancaman siber yang semakin kompleks.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
JULI 2025

Meskipun penting, implementasi program pelatihan dan sertifikasi keamanan siber tidak lepas dari tantangan. Terkadang masih ada kesenjangan antara kebutuhan di lapangan dan materi yang diberikan. Oleh sebab itu, program pelatihan harus relevan dan berkelanjutan, dilengkapi dengan evaluasi dan penyesuaian berkala agar tetap efektif. Kolaborasi dengan institusi pendidikan, pelatihan berbasis peran, dan rekrutmen spesialis keamanan siber dengan latar belakang yang kuat adalah langkah-langkah strategis yang dapat memperkuat kapasitas SDM dalam menghadapi ancaman siber.

Selain itu, pembentukan tim tanggap insiden siber yang responsif sangat penting. Tim ini harus terdiri dari ahli keamanan siber yang terlatih dalam analisis ancaman, forensik digital, dan manajemen insiden. Tim juga perlu dilengkapi dengan prosedur operasi standar (SOP) dan teknologi mutakhir untuk deteksi dan respons insiden. Dengan latihan simulasi yang rutin, tim dapat menjaga kesiapan menghadapi ancaman nyata dan memperkuat pertahanan siber nasional.

Teknologi memainkan peran penting dalam pertahanan siber Koopsudnas, terutama dalam melindungi infrastruktur kritis dan menjaga keamanan operasi militer. Penggunaan teknologi canggih seperti *Intrusion Detection Systems* (IDS), *Intrusion Prevention Systems* (IPS), *firewall*, dan Sistem Informasi dan Manajemen Keamanan (SIEM) dianggap vital untuk mendeteksi aktivitas mencurigakan. Enkripsi dan manajemen kunci yang kuat juga diperlukan untuk melindungi data sensitif. Namun, selain teknologi, pengembangan regulasi dan pelatihan berkelanjutan bagi personel sangat diperlukan untuk meningkatkan efektivitas.

Penerapan teknologi yang canggih juga perlu mudah digunakan agar bisa diterima dengan baik oleh personel. Konsep Penerimaan Teknologi (ITAM) menekankan pentingnya penggunaan teknologi yang *user-friendly* agar implementasinya efektif. Penelitian mendukung bahwa teknologi seperti IDS, IPS, SIEM, dan enkripsi data yang kuat bisa memperkuat sistem pertahanan siber Koopsudnas. Namun, teknologi ini harus relevan dengan kebutuhan operasional dan mampu merespons ancaman yang terus berkembang.

Meskipun teknologi berperan penting dalam pertahanan siber, tantangan tetap ada, seperti kelemahan dalam pengembangan kekuatan militer siber dan regulasi. Oleh karena itu, Koopsudnas harus mengombinasikan teknologi dengan pengembangan regulasi yang kuat dan pelatihan untuk meningkatkan keterampilan personel. Dengan adopsi teknologi baru seperti AI, *open source*, dan pembangunan lab siber, Koopsudnas dapat lebih siap menghadapi ancaman yang semakin kompleks.

Alokasi sumber daya yang memadai sangat penting dalam mendukung strategi pertahanan siber Koopsudnas, mencakup anggaran untuk pengadaan teknologi canggih seperti IDS, IPS, *firewall*, SIEM, dan enkripsi data. Teori Arthur F. Lykke yang menekankan pentingnya keseimbangan antara tujuan, cara, dan alat menunjukkan bahwa tanpa sumber daya yang tepat, tujuan strategis tidak akan tercapai dengan optimal. Oleh karena itu, penting bagi Koopsudnas untuk memastikan anggaran yang cukup untuk mendukung implementasi teknologi yang dibutuhkan.

Selain anggaran, sumber daya manusia yang kompeten juga merupakan elemen penting dalam strategi ini. Rekrutmen spesialis keamanan siber yang berpengalaman serta pelatihan berkelanjutan bagi personel menjadi langkah penting yang sejalan dengan teori Clausewitz tentang pentingnya kualitas personel dalam keberhasilan strategi militer. Pembangunan fasilitas seperti laboratorium siber untuk simulasi dan pengujian juga dibutuhkan untuk mengembangkan keterampilan personel dalam menghadapi ancaman siber, sebagaimana

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
JULI 2025

ditunjukkan dalam penelitian yang menekankan pentingnya fasilitas untuk meningkatkan kesiapan pertahanan.

Koordinasi dan efisiensi penggunaan sumber daya juga harus diperhatikan agar strategi pertahanan siber berjalan efektif. Selain teknologi yang selalu diperbarui, Koopsudnas juga harus memastikan adanya pemeliharaan rutin, audit keamanan, dan pengembangan infrastruktur IT yang kuat. Kolaborasi dengan institusi pendidikan, perusahaan teknologi, dan lembaga pemerintah lain seperti BSSN akan memperkuat strategi ini, memastikan Koopsudnas dapat menghadapi ancaman siber dengan lebih tangguh dan efektif.

Implementasi strategi pertahanan siber di Koopsudnas harus memperhatikan pengelolaan risiko yang efektif, sebagaimana dijelaskan dalam teori kekuatan Hans Morgenthau. Morgenthau menekankan pentingnya keseimbangan antara kekuatan nasional dan alokasi sumber daya untuk menghadapi ancaman. Dalam konteks pertahanan siber, Koopsudnas perlu menjaga keseimbangan antara kemampuan pertahanan yang dimiliki dan sumber daya yang tersedia dengan kebijakan yang realistis dan pragmatis untuk meminimalkan risiko siber.

Samuel P. Huntington juga memberikan pandangan penting mengenai pentingnya regulasi yang kuat dan koordinasi antar lembaga untuk menjaga keamanan nasional. Strategi pertahanan siber Koopsudnas harus memiliki kerangka kerja yang jelas agar semua aspek pertahanan dapat diintegrasikan dengan baik. Tanpa regulasi yang terstruktur, pengelolaan risiko akan sulit dijalankan, sehingga penting bagi Koopsudnas untuk memiliki pendekatan yang terkoordinasi dengan lembaga terkait dalam menghadapi ancaman siber.

Salah satu risiko utama yang dihadapi adalah keterbatasan anggaran, yang dapat menghambat pengadaan teknologi canggih dan pelatihan bagi personel. Manajemen risiko yang baik harus diterapkan untuk mengalokasikan anggaran secara efisien dan memastikan prioritas pada aspek-aspek penting strategi pertahanan siber. Selain itu, perkembangan teknologi serangan siber yang semakin canggih juga menjadi risiko besar, sehingga Koopsudnas perlu terus memperbarui sistem keamanan dan melakukan audit rutin untuk meminimalkan potensi serangan.

Risiko lain yang perlu diperhatikan adalah kesiapan personel dalam menghadapi ancaman siber dan koordinasi antar lembaga. Pelatihan berkelanjutan dan simulasi serangan siber harus diadakan secara rutin untuk meningkatkan pemahaman dan respons personel. Selain itu, komunikasi yang efektif dan kerja sama yang baik antara Koopsudnas dan lembaga pemerintah lainnya seperti BSSN sangat penting untuk mengatasi perbedaan kebijakan dan prosedur antar lembaga, sehingga respons terhadap ancaman siber dapat dilakukan dengan cepat dan efektif.

Strategi pertahanan siber di Koopsudnas yang berbasis pada pendekatan *Ends, Ways, Means,* dan *Risks* menawarkan kerangka kerja yang komprehensif dan terstruktur untuk memperkuat kemampuan pertahanan siber. Tujuan yang jelas, konsep yang efektif, sumber daya yang tepat, dan pengelolaan risiko yang baik adalah kunci untuk memperkuat kemampuan pertahanan siber Koopsudnas. Implementasi strategi ini diharapkan dapat meningkatkan ketahanan siber dan mendukung pertahanan udara nasional yang lebih tangguh, menghadapi ancaman siber yang semakin kompleks dan beragam.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
JULI 2025

5. KESIMPULAN DAN SARAN

Kesimpulan utama dari penelitian ini menunjukkan bahwa Koopsudnas menghadapi beberapa tantangan dalam sistem pertahanan sibernya, seperti keterbatasan personel, regulasi yang belum memadai, dan teknologi yang belum optimal. Keterbatasan sumber daya manusia dengan keahlian khusus di bidang siber menjadi hambatan dalam menghadapi ancaman yang semakin kompleks. Selain itu, regulasi yang ada saat ini belum mencakup semua aspek penting dalam pertahanan siber, terutama terkait dengan manajemen risiko dan respons insiden. Masalah lainnya adalah penggunaan teknologi yang masih terbatas, yang membuat sistem pertahanan udara nasional rentan terhadap serangan siber.

Strategi yang efektif untuk meningkatkan pertahanan siber di Koopsudnas melibatkan penguatan regulasi, peningkatan kualitas personel, dan investasi dalam teknologi canggih. Regulasi yang kuat dan terstruktur harus disertai dengan koordinasi antar lembaga yang lebih baik. Di sisi lain, peningkatan jumlah dan kualitas personel keamanan siber harus didukung dengan program pelatihan dan sertifikasi yang berkelanjutan. Di bidang teknologi, adopsi sistem deteksi intrusi, firewall, enkripsi data, dan pemanfaatan kecerdasan buatan (AI) dapat meningkatkan efektivitas pertahanan siber.

Sebagai rekomendasi, disarankan agar pemerintah Indonesia meningkatkan kerjasama internasional di bidang keamanan siber untuk mengakses teknologi terbaru dan belajar dari praktik terbaik negara lain. Selain itu, TNI AU disarankan untuk meluncurkan program peningkatan kesadaran keamanan siber di seluruh jajaran, melalui pelatihan rutin dan kampanye kesadaran, guna membangun budaya keamanan yang lebih kuat dan mengurangi risiko serangan siber akibat kesalahan manusia.

DAFTAR PUSTAKA

1. Buku

Anwar, S. T. (1998). *Book Review: The Clash of Civilizations and the Remaking of World Order*.

Amalia, F. S., Mahroza, J., Halkis, M., Priyanto, P., Purwanto, S., & Gunawan, R. & David, L.(2024). *Diplomasi Pertahanan Indonesia-Australia untuk Humanitarian Assistance and Disaster Relief (HADR)*.

Arikunto, S. (2010). *Metode peneltian*. Jakarta: Rineka Cipta, 173.

Chandler, D. (2014). *Resilience: The governance of complexity*. Routledge.

Clarke & Knake (2011). *Cyber war: the next threat to national security and what to do about it?* Ecco.

Clausewitz, C. Von. (1976). *Carl Von Clausewitz On War*, (translated by Michael Howard and Peter Paret) (M. H. and P. Paret (ed.)). Princeton University Press

Cuff, E. C., Sharrock, W. W., Framcis, D. W., Dennis, A. J., & Francis, D. W. (2006). *Perspectives in sociology*. Routledge.

Djalal, H. (2015). *Wawasan Nusantara dan Indonesia Global*. Gramedia Pustaka Utama.

Douhet, G. (2009). *The Command of The Air*. University of Alabama Press.

Everett M. Rogers. (2003). *Diffusion of Innovations*, 5th Edition. Free Press.

Farizy, Salman. (2020). *Keamanan Sistem Informasi*. Unpam Press. Jakarta

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
JULI 2025

Geoffrey A. Moore. (1991). *Crossing the Chasm: Marketing and Selling High-Tech Products to Mainstream Customers*. Harper Business.

Hart, B. L. (2014). *Strategy: the indirect approach*. In Strategic Studies (pp. 101-104). Routledge.

Hinnebusch, R, 2007. *The US invasion of Iraq: Explanations and implications*. Critique: Critical Middle Eastern Studies

Jervis, R. (2020). *The Illogic of American nuclear strategy*. Cornell University Press

Miles, Huberman, & Saldana (2014). Qualitative Data Analysis.

Mawardi, M. C., Sutanto, R., & Purwanto, S. (2025). Strategy to Improve the Calibration Capability of Depohar 20 to Ensure the Quality of Maintenance Results in Supporting the Readiness of the Air Force's Defense System. *Formosa Journal of Applied Sciences*, *4*(7), 2165-2178.

Moleong, L. J., & Edisi, P. R. R. B. (2004). *Metodelogi penelitian*. Bandung: Penerbit Remaja Rosdakarya, 3(01).

Moleong, L. J. (2017). *Metodologi penelitian kualitatif* edisi revisi.

Morgenthau H. J. (1973). *Politics among nations: the struggle for power and peace* (5th ed.). Alfred A. Knopf.

M. Sobry Sutikno,(2020), *Penelitian Kualitatif* (Lombok:Holistica,)

Sanger, D. E. (2017). *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Crown.

Scarfone, K., Jansen, W., & Tracy, M. (2008). *Guide to general server security*. NIST Special Publication, 800(123).

Purwanto, S., Ardiansyah, M., Januru, L., Anami, Z., Putri, N. A. S. M., Gunadi, I., ... & Hastriana, U. S. (2025). *Pengembangan Karier dan Kompetensi SDM*. Yayasan Tri Edukasi Ilmiah.

Purwanto, S., Supangat, S., Esterina, M., Souhoka, S., Chandra, F., & Hariputra, A. & Arianto, T.(2024). *Manajemen Sumber Daya Manusia. Yayasan Tri Edukasi Ilmiah*.

Schelling, T. C. (2020). *Arms and Influence*, rev. ed.(1966; repr., New Haven, CT.

Sugiyono. (2016). *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Bandung: PT Alfabet.

Waltz, K. N. (2010). *Theory of international politics*. Waveland Press.

Zed, M. (2008). *Metode penelitian kepustakaan*. Yayasan Pustaka Obor Indonesia.

2. Jurnal

Arthur F. Lykke, Jr (1997) *Defining Militery Strategy*. Militery Review. January-Februari. PP. 183-186

Denning, D. E. (2014). *Framework and principles for active cyber defense*. Computers & Security, 40, 108-113.

Hironimus-Wendt, R. J., & Wallace, L. E. (2009). *The sociological imagination and social responsibility*. Teaching Sociology, 37(1), 76-88.

Kaelan, M. (2018). *Pancasila Sebagai Ideologi Nasional dan Pedoman Berperilaku Bagi Prajurit TNI*. Jurnal Pertahanan dan Keamanan, 4(1)

Keith, A., & Ahner, D. (2021). *Counterfactual regret minimization for integrated cyber and air defense resource allocation*. European Journal of Operational Research, 292(1), 95-107.

Keohane, R. O., & Nye Jr, J. S. (1973). *Power and interdependence*. Survival, 15(4), 158-165.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
JULI 2025

Krisnata, R., Reksoprodjo, A. H., & Waluyo, S. D. (2022). *Strategi Pengembangan Kapabilitas Siber Pertahanan Untuk Menghadapi Peperangan Siber (Studi Kasus Pada PUSHANSIBER KEMHAN RI 2020-2021)*. NUSANTARA: Jurnal Ilmu Pengetahuan Sosial, 9(6), 2094-2103

Lestari, F. (2016). *Implementasi Tugas dan Fungsi TNI dalam Mewujudkan Pertahanan Negara yang Tangguh dan Mandiri Berdasarkan UUD 1945*. Jurnal Ilmu Hukum, 10(2)

Piercy, N., & Giles, W. (1989). *Making SWOT Analysis Work*. Marketing Intelligence & Planning, 7(5/6), 5-7.

Purwanto, S., Hidayatullah, S. S. W., & Tirtoadisuryo, D. HUMAN RESOURCE DEVELOPMENT STRATEGIES FOR ENHANCING ORGANIZATIONAL PERFORMANCE IN THE DIGITAL ERA.

Purwanto, S., & Ilhamsyah, I. (2025). Army Human Resources Development Strategy through Human Capital Approach. *Indonesian Journal of Social Science and Education (IJOSSE)*, *1*(1), 1-22.

Savitri, R. N. R., & Prabandari, A. P. (2020). *TNI Angkatan Udara dan Keamanan Wilayah Udara Indonesia*. Jurnal Pembangunan Hukum Indonesia, 2(2), 236-245.

Subiyanto, B. (2013). *Perkembangan Konsep Ketahanan Nasional di Indonesia.* Jurnal Ilmiah Peuradeun, 1(2).

Waruwu, E., Purwanto, S., & Widodo, M. D. A. (2025). Strategi Pembinaan Mental Tradisi Kejuangan Prajurit Terhadap Situasi Global Guna Mendukung Tugas TNI AU. *Journal of Law & Policy Review*, *3*(1), 109-118.

3. Media Internet

Badan Siber dan Sandi Negara (BSSN). (2020). *Laporan Tahunan Insiden Siber*. Retrieved from https://www.bssn.go.id/laporan-tahunan.

Davis, F. D. (1985). *A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results* (Doctoral dissertation, Massachusetts Institute of Technology).

FireEye. (2019). *APT Threat Report*. Retrieved from https://www.fireeye.com/current-threats/apt-reports.html

Gartner. (2020). *Use AI and Machine Learning to Enhance Your Security*. Retrieved from https://www.gartner.com/en/documents/4002135/use-ai-and-machine-learning-to-enhance-your-security

https://bssn.go.id/annualreport2022/ Diunduh tanggal 19 Maret 2024 pukul 10:14 WIB

https://swa.co.id/swa/trends/technology/waspada-tren-serangan-siber-di-2023-lebih-mutakhir Diunduh tanggal 19 Maret 2024 pukul 10:23 WIB

(ISC)². (2019). *Cybersecurity Workforce Study*. Retrieved from https://www.isc2.org/Research/Workforce-Study

Kemp, Simon. (2023). *Digital 2023: Indonesia*. https://datareportal.com/reports/digital-2023-indonesia. Diunduh tanggal 19 Maret 2024.

Nasya Lingga Carissa (2024) *Clausewitz dan Konsep Strategi: Perang Sebagai Keberlanjutan Politik*. diunduh dari laman: https://www.researchgate.net/publication/377976545_Clausewitz_dan_Konsep_Strategi_Perang_Sebagai_Keberlanjutan_Politik

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email:admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 1
JULI 2025

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf