QISTINA: Jurnal Multidisiplin Indonesia
P-ISSN: 2964-6278 E-ISSN: 2964-1268
Vol. 4 No. 2 Desember 2025

Strategi Pertahanan TNI AD Dalam Menghadapi Ancaman Siber (Studi Kasus Perang Rusia-Ukraina Periode 2014-2023)

Suwanda[1] Deni Dadang AR[2] Dwi Hartono[3]
Strategi Pertahanan Darat, Strategi Pertahanan, Universitas Pertahanan RI, Jakarta[1,2,3]
Email: wandachb@gmail.com[1] denidar63@gmail.com[2] dwihartono11328@gmail.com[3]

Abstrak

Ruang siber kini menjadi elemen penting dalam pertahanan modern. Perang Rusia-Ukraina periode 2014-2023 menunjukkan bahwa serangan siber dapat terintegrasi dengan operasi militer untuk merusak infrastruktur vital, mengganggu sistem komando dan komunikasi, serta menyebarkan disinformasi. Di Indonesia, berbagai anomali dan insiden siber terjadi pada instansi strategis, termasuk TNI AD, seperti kebocoran data, serangan malware, *website defacement*, dan serangan siber lainnya, menunjukkan bahwa ancaman terhadap pertahanan nasional semakin nyata dan perlu mendapat perhatian serius. Oleh karena itu, TNI AD perlu memperkuat pertahanan siber yang adaptif dan berlapis guna menjaga jaringan komando, sistem informasi, dan kesiapsiagaan operasional. Penelitian ini bertujuan menganalisis kesiapan TNI AD dalam menghadapi ancaman siber, mengidentifikasi faktor internal dan eksternal yang mempengaruhi pembangunan pertahanan siber, serta merumuskan strategi yang dapat diterapkan menggunakan kerangka *Ends, Ways,* dan *Means.* Metode penelitian bersifat deskriptif kualitatif melalui pendekatan studi kasus Perang-Ukraina periode 2014-2023. Hasil penelitian menunjukkan bahwa TNI AD telah memiliki satuan siber dan infrastruktur teknologi dasar. Namun, masih terdapat tantangan berupa ketimpangan infrastruktur teknologi antar satuan, keterbatasan personel ahli yang tersertifikasi, implementasi regulasi yang belum konsisten, serta koordinasi lintas lembaga yang perlu diperkuat. Pembelajaran dari perang Rusia–Ukraina menekankan pentingnya struktur komando siber yang kuat, SDM profesional, pertahanan berlapis, integrasi C5ISR, serta kemandirian teknologi. Kesimpulannya, pertahanan siber TNI AD masih dalam tahap berkembang dan membutuhkan penguatan organisasi, SDM, infrastruktur teknologi, serta tata kelola. Diperlukan pemerataan kapasitas siber, peningkatan profesionalisme personel, modernisasi infrastruktur teknologi, serta kolaborasi nasional untuk mewujudkan pertahanan siber yang adaptif dan tangguh.

Kata Kunci: *Rusia–Ukraina, Pertahanan Siber, Kerangka Ends, Ways, Means*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mengubah lanskap ancaman keamanan negara secara fundamental. Ancaman tidak lagi terbatas pada agresi fisik dan konvensional, tetapi berkembang ke dalam ruang siber yang bersifat asimetris, lintas batas, dan berdampak sistemik. Dalam konteks ini, ancaman siber telah menjadi isu strategis yang berimplikasi langsung terhadap keamanan nasional, stabilitas pemerintahan, serta efektivitas operasi militer. Budiman Dwi Cahyo et al. (2023) menegaskan bahwa ruang siber kini tidak hanya berfungsi sebagai pendukung operasi militer, tetapi telah bertransformasi menjadi domain strategis tersendiri dalam konflik modern. Konflik Rusia–Ukraina periode 2014–2023 memberikan gambaran empiris yang jelas mengenai peran strategis siber dalam peperangan kontemporer. Sejak aneksasi Krimea pada 2014 hingga invasi militer skala penuh pada 2022, Ukraina menghadapi rangkaian serangan siber yang terkoordinasi dengan operasi militer konvensional. Serangan tersebut menyasar infrastruktur informasi vital, seperti sistem energi, komunikasi, transportasi, keuangan, dan pemerintahan, melalui penggunaan malware, wiper, distributed denial of service (DDoS), serta operasi spionase dan disinformasi digital. Pola ini menunjukkan bahwa serangan siber dirancang untuk melumpuhkan fungsi negara,

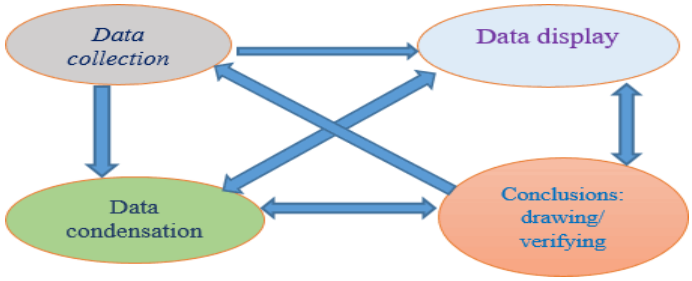
mengganggu sistem komando dan kendali, serta melemahkan ketahanan nasional secara menyeluruh (Budiman Dwi Cahyo et al., 2023).

Selain berdimensi teknis, perang siber dalam konflik Rusia–Ukraina juga menonjolkan dimensi psikologis dan informasi. Operasi disinformasi dan propaganda digital digunakan untuk menciptakan disorientasi informasi, menurunkan moral masyarakat sipil, serta mempengaruhi persepsi publik domestik dan internasional. Intensitas serangan yang terjadi secara berkelanjutan menjadikan Ukraina sebagai arena uji coba berbagai taktik dan teknik perang siber modern. Kondisi ini menegaskan bahwa dominasi ruang siber telah menjadi faktor kunci dalam pencapaian tujuan militer dan politik pada konflik bersenjata masa kini. Pembelajaran dari perang Rusia–Ukraina memberikan sejumlah pelajaran penting bagi Indonesia. Pertama, konflik tersebut menunjukkan bahwa pertahanan siber harus diposisikan sebagai bagian integral dari sistem pertahanan nasional dan operasi militer, bukan sekadar fungsi teknis pendukung. Integrasi antara operasi siber dan operasi konvensional menjadi prasyarat bagi efektivitas sistem komando dan kendali modern. Kedua, kejelasan struktur komando siber dan koordinasi lintas sektor terbukti berpengaruh terhadap kecepatan respons dan efektivitas penanganan serangan siber. Fragmentasi kelembagaan dan regulasi pada tahap awal konflik Ukraina justru memperbesar kerentanan terhadap serangan (Budiman Dwi Cahyo et al., 2023). Ketiga, perang Rusia–Ukraina menegaskan pentingnya penguatan sumber daya manusia siber dan kolaborasi nasional. Ukraina mampu meningkatkan ketahanan sibernya dengan melibatkan komunitas teknologi informasi dan profesional sipil sebagai bagian dari upaya pertahanan nasional. Sebaliknya, ketergantungan tinggi pada teknologi dan infrastruktur asing pada fase awal konflik meningkatkan kerentanan terhadap eksploitasi dan sabotase siber (Anjelina, 2023). Pelajaran ini relevan bagi Indonesia untuk mendorong kemandirian teknologi siber secara bertahap serta membangun ekosistem pertahanan siber nasional yang berkelanjutan.

Selanjutnya bagaimana kondisi di Indonesia, relevansi pembelajaran tersebut diperkuat oleh tingginya ancaman siber di masa damai. Laporan Badan Siber dan Sandi Negara (BSSN) mencatat ratusan juta trafik anomali siber sepanjang tahun 2024, sementara di lingkungan Tentara Nasional Indonesia Angkatan Darat (TNI AD) tercatat puluhan ribu anomali dan insiden siber dengan tingkat dampak yang beragam (BSSN, 2024; Pussansiad, 2024). Fakta ini menunjukkan bahwa risiko gangguan terhadap stabilitas nasional dan keamanan operasional militer melalui ruang siber bersifat nyata dan berkelanjutan. Sebagai bagian dari sistem pertahanan negara, TNI AD dituntut memiliki kapabilitas pertahanan siber yang adaptif dan tangguh. Secara normatif, penanggulangan ancaman siber telah menjadi bagian dari tugas TNI melalui kerangka operasi militer selain perang, serta diperkuat dengan pembentukan satuan sandi dan siber. Namun, berbagai kajian terdahulu menunjukkan bahwa pembangunan pertahanan siber TNI AD masih menghadapi tantangan dalam aspek sumber daya manusia, infrastruktur teknologi, regulasi, dan koordinasi lintas lembaga (Sarjito, 2024). Tantangan tersebut menuntut adanya evaluasi strategis yang sistematis dan berorientasi jangka panjang. Berdasarkan kondisi tersebut, penelitian ini bertujuan menganalisis strategi pertahanan siber TNI AD dengan menggunakan kerangka *Ends, Ways, dan Means* yang dipopulerkan oleh Arthur F. Lykke Jr (1989). Kerangka ini digunakan untuk menilai keterkaitan antara tujuan strategis (*Ends*), pendekatan operasional (*Ways*), dan sumber daya (*Means*) yang dimiliki dalam menghadapi ancaman siber. Pembelajaran dari perang Rusia–Ukraina dijadikan referensi empiris untuk merumuskan rekomendasi strategis yang kontekstual dan aplikatif bagi penguatan pertahanan siber TNI AD, guna menghadapi dinamika ancaman multidimensi di masa depan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan desain studi kasus untuk menganalisis strategi pertahanan siber TNI AD dalam menghadapi ancaman siber, berdasarkan pembelajaran perang Rusia–Ukraina periode 2014–2023. Pendekatan ini dipilih untuk memperoleh pemahaman mendalam terhadap fenomena strategis yang bersifat kompleks dan kontekstual. Penelitian dilaksanakan di Pusat Sandi dan Siber TNI AD (Pussansiad) pada periode Mei–November 2025. Informan ditentukan melalui purposive sampling, terdiri atas personel TNI AD yang memiliki peran strategis di bidang siber, serta akademisi dan praktisi keamanan siber dari kalangan sipil guna mendukung triangulasi dan mengurangi bias institusional. Objek penelitian mencakup kesiapan TNI AD, faktor-faktor yang mempengaruhi, serta strategi pertahanan siber yang diterapkan. Pengumpulan data dilakukan melalui wawancara mendalam, studi dokumen, dan observasi tidak langsung. Teknik pengolahan data dilakukan untuk menjamin keabsahan data melalui uji kredibilitas, transferabilitas, dependabilitas, dan konfirmabilitas. Sedangkan analisis data dilakukan menggunakan model analisis interaktif Miles, Huberman, dan Saldana (2014) yang meliputi kondensasi data, penyajian data, serta penarikan dan verifikasi kesimpulan secara berulang. Berikut gambar model analisis interaktif Miles, Huberman, dan Saldana (2014);



Gambar 1. Model Analisis Interaktif
Sumber: Miles, Huberman, dan Saldana (2014)

HASIL PENELITIAN DAN PEMBAHASAN

Wawancara

Hasil wawancara menunjukkan bahwa informan dari internal TNI AD maupun kalangan sipil memiliki pandangan yang relatif sejalan mengenai kondisi pertahanan siber TNI AD. Secara umum, tujuan strategis pertahanan siber telah dipahami dengan baik, terutama dalam menjaga keamanan sistem informasi dan keberlangsungan fungsi komando dan kendali. Namun, pencapaian tujuan tersebut masih memerlukan penguatan pada aspek pendekatan operasional dan ketersediaan sumber daya. Para informan menekankan pentingnya penegasan struktur organisasi siber, integrasi fungsi siber ke dalam sistem C5ISR (*Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance*), serta peningkatan kemampuan deteksi dini, respons, dan pemulihan insiden. Selain itu, karakter ancaman siber yang bersifat simultan dan terkoordinasi, sebagaimana terlihat dalam perang Rusia–Ukraina, menuntut respons yang cepat dan terpusat. Dari sisi sumber daya, keterbatasan SDM siber profesional, ketimpangan infrastruktur, dan ketergantungan teknologi masih menjadi faktor yang perlu diperkuat agar efektivitas pertahanan siber TNI AD dapat terus ditingkatkan.

Studi Dokumen

Studi dokumen dilakukan untuk menelaah kebijakan dan pedoman operasional pertahanan siber TNI AD guna memahami tujuan strategis, pendekatan operasional, dan

dukungan sumber daya yang dirancang. Hasil kajian digunakan untuk menilai keselarasan antara kebijakan dan praktik, serta sebagai pembanding terhadap temuan wawancara dan observasi. Hasil studi dokumen menunjukkan bahwa implementasi kebijakan pertahanan siber masih memerlukan penguatan agar lebih selaras dengan perkembangan ancaman dan kapasitas sumber daya, sehingga tujuan strategis dapat dicapai secara optimal.

Observasi

Hasil observasi menunjukkan bahwa mekanisme deteksi dan pemantauan ancaman siber di lingkungan TNI AD telah berjalan dan mampu mengidentifikasi anomali jaringan melalui pusat operasi dan sistem pemantauan yang tersedia. Namun, efektivitas respons dan pemulihan masih memerlukan penguatan, terutama terkait integrasi sistem, pemerataan perangkat keamanan, dan kesiapan personel di tingkat satuan. Temuan ini menegaskan bahwa optimalisasi sumber daya dan integrasi operasional menjadi kunci dalam memperkuat ketahanan siber TNI AD secara menyeluruh.

Pembahasan

Pada bagian pembahasan ini menguraikan hasil analisis mengenai kesiapan TNI AD dalam menghadapi ancaman siber, faktor-faktor yang mempengaruhi pembangunan strategi pertahanan siber, serta perumusan strategi pertahanan siber TNI AD berdasarkan pembelajaran perang Rusia–Ukraina periode 2014–2023. Pembahasan disusun melalui triangulasi data yang melibatkan hasil pengumpulan, analisis, dan interpretasi data secara sistematis, sehingga memberikan gambaran komprehensif mengenai kondisi aktual pertahanan siber TNI AD dan implikasinya bagi pengembangan strategi ke depan.

Kesiapan TNI AD dalam menghadapi ancaman siber di era digital saat ini

Kesiapan TNI AD dalam menghadapi ancaman siber di era digital perlu dipahami secara komprehensif melalui kesiapan organisasi, sumber daya manusia, infrastruktur dan teknologi, serta regulasi dan kebijakan yang mendasarinya. Keempat aspek ini menjadi elemen kunci yang menentukan kemampuan TNI AD dalam membangun pertahanan siber yang efektif dan berkelanjutan.

a. Kesiapan Organisasi

Kesiapan organisasi TNI AD dalam menghadapi ancaman siber ditunjukkan melalui pembentukan Pussansiad, Kartika CSIRT (*Computer Security Incident Response Team*), dan CSOC (*Cyber Security Operation Center*) sebagai fondasi pertahanan siber. Dalam kerangka *Ends*, langkah ini mencerminkan tujuan strategis untuk melindungi sistem informasi dan komando sebagai pusat gravitasi pertahanan modern. Dari sisi *Ways*, keberadaan CSIRT dan CSOC menunjukkan penerapan mekanisme deteksi, pemantauan, dan penanganan insiden siber, meskipun pelaksanaannya masih terpusat dan belum merata di seluruh satuan. Sementara itu, pada aspek Means, keterbatasan pemerataan infrastruktur, validasi organisasi, dan SDM siber menunjukkan bahwa dukungan sumber daya belum sepenuhnya selaras dengan tujuan dan pendekatan yang telah dirumuskan. Ketidakseimbangan ini menempatkan kesiapan organisasi TNI AD pada tahap berkembang dan memerlukan penguatan terintegrasi agar strategi pertahanan siber dapat berjalan lebih efektif.

b. Kesiapan Sumber Daya Manusia (SDM)

Kesiapan sumber daya manusia TNI AD dalam menghadapi ancaman siber menunjukkan bahwa institusi telah memiliki personel dengan kemampuan dasar di bidang siber untuk mendukung perlindungan sistem informasi pertahanan. Dari sisi *Ends*, pengembangan SDM siber diarahkan untuk menjaga keamanan informasi dan memastikan

keberlangsungan fungsi komando dan kendali. Pada aspek *Ways*, peningkatan kemampuan dilakukan melalui pendidikan dan pelatihan, serta penugasan personel pada unit-unit siber yang relevan. Namun, pelaksanaannya masih terbatas dan belum merata di seluruh satuan. Sementara itu, pada aspek *Means*, jumlah personel dengan keahlian siber masih terbatas, distribusinya belum merata, dan pola pembinaan serta jalur karier siber masih perlu diperkuat. Kondisi ini menunjukkan bahwa kesiapan SDM TNI AD masih berada pada tahap berkembang dan memerlukan penguatan yang lebih terencana agar mampu menjawab tantangan ancaman siber yang semakin kompleks.

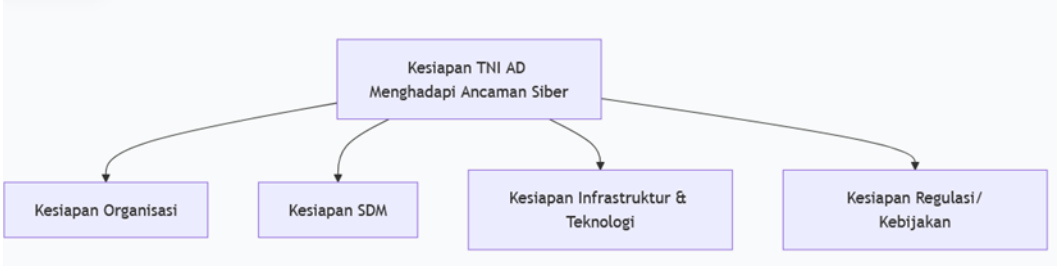
c. Kesiapan Infrasrtuktur & Teknologi

Kesiapan infrastruktur dan teknologi TNI Angkatan Darat dalam menghadapi ancaman siber menunjukkan bahwa institusi telah memiliki dukungan awal yang penting bagi penyelenggaraan pertahanan siber. Dari sisi *Ends*, pengembangan infrastruktur dan teknologi diarahkan untuk melindungi sistem informasi, jaringan komunikasi, serta mendukung keberlangsungan fungsi komando dan kendali. Pada aspek *Ways* infrastruktur dan teknologi siber dimanfaatkan untuk pemantauan jaringan, deteksi dini, dan penanganan insiden. Namun, pemanfaatannya masih terpusat dan belum terintegrasi secara merata di seluruh satuan, sehingga efektivitas respons belum optimal. Sedangkan sisi *Means,* infrastruktur dan teknologi masih memerlukan penguatan, khususnya dalam pemerataan perangkat, peningkatan kapasitas sistem, dan integrasi antar satuan. Kondisi ini menunjukkan bahwa dukungan teknologi TNI AD masih berada pada tahap berkembang dan perlu ditingkatkan secara berkelanjutan agar selaras dengan tuntutan ancaman siber yang semakin kompleks.

d. Kesiapan Regulasi/Kebijakan

Kesiapan regulasi dan kebijakan TNI AD dalam menghadapi ancaman siber menunjukkan bahwa institusi telah memiliki landasan hukum dan pedoman dasar yang mendukung penyelenggaraan pertahanan siber. Dari sisi *Ends*, regulasi dan kebijakan diarahkan untuk menjamin keamanan informasi dan keberlangsungan sistem komando dan kendali. Pada aspek *Ways*, kebijakan internal, SOP, dan pedoman teknis menjadi acuan pelaksanaan pengamanan sistem dan penanganan insiden siber di lingkungan TNI AD. Sementara itu, pada aspek *Means*, implementasi regulasi masih memerlukan penguatan agar dapat diterapkan secara konsisten dan merata di seluruh satuan. Hal ini menunjukkan bahwa kesiapan regulasi dan kebijakan TNI AD berada pada tahap berkembang dan memerlukan penyelarasan berkelanjutan agar mampu mendukung efektivitas pertahanan siber secara menyeluruh.

Secara umum dapat disimpulkan bahwa TNI AD telah memiliki fondasi awal berupa struktur organisasi siber, regulasi dasar, sumber daya manusia dengan kompetensi awal, serta dukungan infrastruktur dan teknologi. Namun, kesiapan tersebut belum sepenuhnya terintegrasi dan merata di seluruh satuan. Keterbatasan pemerataan kapasitas, integrasi operasional, serta penguatan SDM dan infrastruktur menunjukkan bahwa kesiapan siber masih memerlukan peningkatan berkelanjutan agar selaras dengan dinamika ancaman siber yang semakin kompleks dan terkoordinasi. Untuk memudahkan pemahaman panalisis pembahasan di atas, berikut di bawah ini gambar dan tabel pemetaan kesiapan TNI AD dalam menghadapi ancaman siber di era digital saat ini menurut kerangka *Ends, Ways, Means.*



Gambar 2. Pemetaan Kesiapan TNI AD dalam menghadapi ancaman siber di era digital saat ini

Tabel 1. Pemetaan Kerangka *Ends, Ways, Means* pada kesiapan TNI AD

No	Aspek Kesiapan	*Kerangka Ends, Ways, Means*	Data temuan di lapangan
1	**2**	***3***	**4**
1.	Organisasi	*Ends*	Struktur Pussansiad, Kartika CSIRT TNI AD mencerminkan tujuan strategis TNI AD dalam membangun postur pertahanan siber yang terpusat dan kuat.
		Ways	Pembentukan unit pelaksana siber, penetapan alur komando, penguatan koordinasi antar-satuan, dan pengaturan fungsi teknis sebagai mekanisme operasional pertahanan siber TNI AD.
		Means	Ketidakrataan struktur dan kapasitas antar satuan menunjukkan sumber daya kelembagaan belum mendukung tujuan secara merata.
2.	Sumber Daya Manusia (SDM)	*Ends*	tersedianya personel yang kompeten, tersertifikasi, dan mampu menjalankan operasi pertahanan siber secara efektif di seluruh satuan TNI AD.
		Ways	Pelatihan, penugasan teknis, dan program peningkatan kapasitas menjadi cara untuk memperkuat kemampuan personel di bidang siber.
		Means	Kompetensi dan pemerataan tenaga ahli masih terbatas sehingga belum sepenuhnya mendukung pelaksanaan strategi siber.
3.	Infrastruktur & Teknologi	*Ends*	Infrastruktur berfungsi melindungi dan menjaga keberlangsungan sistem informasi sebagai tujuan strategis organisasi.
		Ways	Pemanfaatan CSOC, SIEM, XDR, dan sensor jaringan menjadi langkah operasional untuk mencapai kemampuan deteksi dan respons yang optimal.
		Means	Ketersediaan perangkat, sistem deteksi, dan pemantauan jaringan belum merata di seluruh satuan
4.	Regulasi & Kebijakan	*Ends*	Terciptanya tata kelola pertahanan siber yang terstandar, konsisten, dan efektif di seluruh satuan TNI AD
		Ways	SOP, pedoman pengamanan, dan kebijakan penggunaan sistem menjadi mekanisme operasional yang mengarahkan pelaksanaan pertahanan siber
		Means	Implementasi regulasi belum konsisten karena pemahaman dan sumber daya pendukung antar satuan masih beragam.

Sumber : data diolah peneliti (2025)

Faktor-Faktor yang Mempengaruhi Strategi Pertahanan Siber TNI AD

Faktor Internal

1. Kekuatan

Faktor internal berupa kekuatan TNI AD menunjukkan adanya fondasi awal yang mendukung pembangunan strategi pertahanan siber. Keberadaan struktur organisasi seperti Pussansiad dan Kartika CSIRT mencerminkan kejelasan tujuan strategis *Ends* dalam melindungi sistem komando dan informasi. Dukungan infrastruktur awal berupa CSOC, SIEM, dan SOAR memungkinkan pelaksanaan fungsi deteksi dan penanganan insiden *Ways*,

sementara ketersediaan personel dengan kompetensi teknis dasar serta regulasi awal menjadi penopang sumber daya (means) dalam penyelenggaraan pertahanan siber.

2. Kelemahan

Di sisi lain, faktor internal berupa kelemahan yaitu sejumlah keterbatasan yang mempengaruhi efektivitas strategi. Struktur dan fungsi siber belum tersedia secara merata di seluruh satuan, jumlah SDM siber tersertifikasi masih terbatas, serta infrastruktur keamanan belum terdistribusi secara seragam. Selain itu, penerapan SOP dan tata kelola belum sepenuhnya konsisten. Kelemahan pada aspek *Means* ini membatasi optimalisasi *Ways* dan menciptakan kesenjangan kapasitas respons antar satuan.

Faktor Eksternal

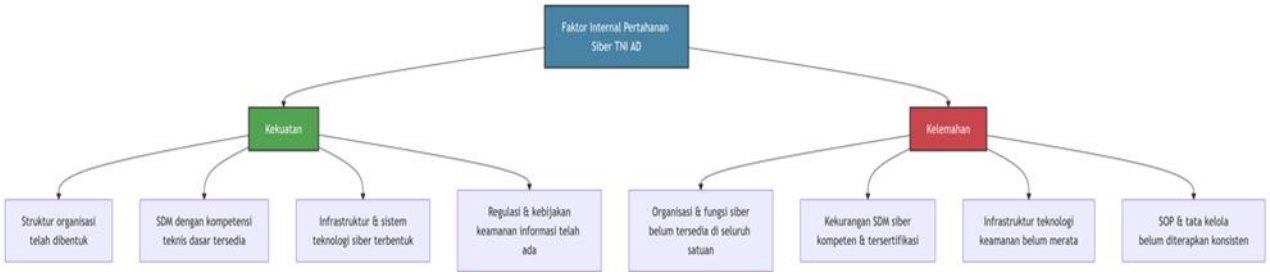
1. Peluang

Lingkungan eksternal menyediakan peluang strategis bagi penguatan pertahanan siber TNI AD. Perkembangan teknologi digital, dukungan kebijakan nasional, kerja sama internasional, serta pembelajaran dari perang Rusia–Ukraina memberikan acuan untuk memperkuat mekanisme operasional (*Ways*) dan memperjelas arah tujuan strategis (*Ends*), khususnya integrasi pertahanan siber dengan operasi militer dan sistem C5ISR.

2. Ancaman

Sebaliknya, faktor eksternal juga menghadirkan ancaman yang signifikan, seperti meningkatnya intensitas serangan siber global, eskalasi geopolitik di kawasan Indo-Pasifik, ketergantungan pada perangkat asing, serta perang informasi. Ancaman ini menuntut kesiapan sumber daya (*Means*) yang lebih kuat dan pendekatan operasional (*Ways*) yang adaptif agar tujuan strategis pertahanan siber dapat tercapai secara berkelanjutan.

Secara umum dapat disimpulkan, bahwa faktor internal dan eksternal membentuk dinamika strategis yang mempengaruhi efektivitas strategi pertahanan siber TNI AD. Kekuatan internal dan peluang eksternal telah mendukung perumusan tujuan (*Ends*) dan sebagian pendekatan operasional (*Ways*), namun kelemahan internal dan ancaman eksternal menunjukkan perlunya penguatan kapasitas sumber daya agar keseimbangan *Ends–Ways–Means* dapat tercapai secara optimal. Untuk memudahkan pemahaman panalisis pembahasan di atas, berikut di bawah ini gambar dan tabel pemetaan faktor internal dan eksternal dalam pertahanan siber TNI AD menurut kerangka *Ends, Ways, Means.*



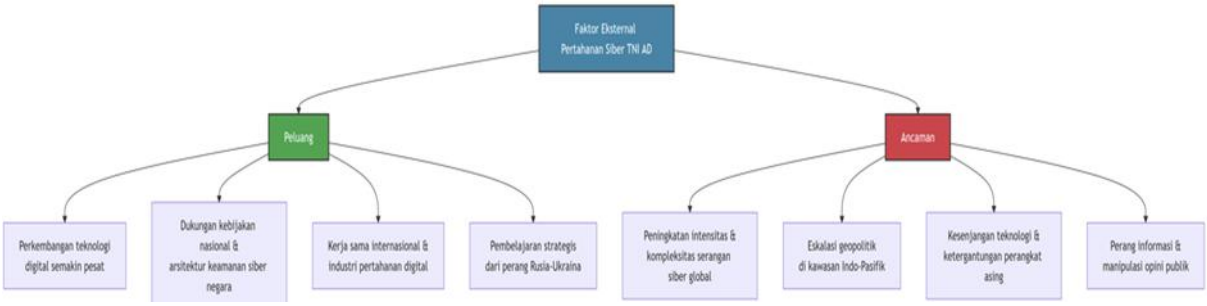
Gambar 3. Faktor Internal yang mempengaruhi pertahanan siber TNI AD
Sumber : data diolah peneliti (2025)

Tabel 2. Pemetaan Faktor Internal pada kerangka Ends, Ways, Means

No	Faktor Internal	Aspek	Kerangka Ends, Ways Means	Data temuan di lapangan
1	2	3	4	5
1.	Kekuatan	Struktur Organisasi telah dibentuk	*Ends*	Struktur Organisasi Pussansiad dan Kartika CSIRT telah dibentuk & sudah melaksanakan fungsinya.

		Tersedia SDM dengan kompetensi teknis dasar	*Means*	Sebagian personel mampumelaksanakan monitoring insiden, konfigurasi jaringan pada tingkat dasar.
		Infrastruktur dan sistem teknologi siber telah terbentuk	*Ways*	CSOC, SIEM & SOAR, Sistek lainnya mampu melaksanakan monitoring *realtime* dan deteksi anomali
		Regulasi dan kebijakan keamanan informasi telah ada	*Ways*	Piranti lunak seperti Juknis. Jukgar, dan SOP lainnya telah tersedia.
2	Kelemahan	Organisasi dan fungsi siber belum tersedia di seluruh satuan TNI AD	*Means*	Satuan di tingkat Kotama/Balakpus fungsi siber masih terbatas, sehingga kapasitas & kapabiltias siber masih terbatas.
		Kekurangan SDM siber yang kompeten dan tersertifikasi	*Means*	Sertifikasi siber & IT lainnya seperti CEH, CHFI & lainnya masih terbatas.
		Infrastruktur teknologi keamanan belum merata di satuan	*Means*	Perangkat proteksi, sensor ancaman, dan fasilitas monitoring belum tersedia di seluruh Kotama/Balakpus.
		SOP dan tata kelola belum diterapkan secara konsisten	*Means*	Perbedaan pemahaman SOP dan keterbatasan sumber daya menyebabkan implementasi tidak seragam.

Sumber : data diolah peneliti (2025)



Gambar 4. Faktor Eksternal yang mempengaruhi pertahanan siber TNI AD
Sumber : data diolah peneliti (2025)

Tabel 3. Pemetaan Faktor Eksternal pada kerangka Ends, Ways, Means

No	Faktor Eksternal	Aspek	Kerangka Ends, Ways Means	Data penelitian sebagai temuan di lapangan
1	**2**	**3**	**4**	**5**
1.	Peluang	Perkembangan teknologi digital semakin pesat	*Ways*	Teknologi baru seperti *AI, Big Data, Machine Learning*, *Zero Trust*, mempercepat deteksi, meningkatkan akurasi respons, dan memperkuat C5ISR.
		Dukungan kebijakan nasional dan arsitektur keamanan siber negara	*Ends*	Kebijakan nasional memberi arah dan standar keamanan siber yang dapat diadopsi TNI AD

		Kerja sama internasional dan industri pertahanan digital	*Ways*	Kerja sama memperkuat kompetensi SDM dan modernisasi perangkat melalui transfer teknologi.
		Pembelajaran strategis dari perang Rusia–Ukraina	Ends	Perang menunjukkan pentingnya integrasi operasi siber dan konvensional serta perlindungan C5ISR.
2.	Ancaman	Peningkatan intensitas dan kompleksitas serangan siber global	*Means*	Serangan multivektor seperti ransomware, DDoS, dan supply-chain semakin menargetkan sektor pertahanan.
		Eskalasi geopolitik di kawasan Indo-Pasifik	*Ends*	Rivalitas kekuatan besar meningkatkan risiko spionase dan infiltrasi jaringan pertahanan.
		Kesenjangan teknologi dan ketergantungan perangkat asing	*Means*	Masih ketergantungan pada perangkat asing menimbulkan risiko backdoor dan kerentanan sistem.
		Perang informasi dan manipulasi opini publik secara konsisten	*Ways*	Serangan informasi dan propaganda digital berpotensi memengaruhi persepsi dan stabilitas operasi militer.

Sumber : data diolah peneliti (2025)

Strategi Pertahanan Siber TNI AD berdasarkan pembelajaran Perang Rusia–Ukraina periode 2013-2024

Pembelajaran dari perang Rusia–Ukraina menunjukkan bahwa operasi siber telah menjadi instrumen strategis yang terintegrasi dengan operasi militer konvensional. Serangan terhadap sistem komando, komunikasi, infrastruktur kritis, dan ruang informasi digunakan untuk menciptakan disrupsi strategis sebelum dan selama operasi fisik berlangsung. Oleh karena itu, strategi pertahanan siber TNI AD perlu dirumuskan secara komprehensif dengan menjaga keseimbangan antara tujuan strategis (*Ends*), pendekatan operasional (*Ways*), dan sumber daya pendukung (*Means*).

a. Penguatan Struktur dan Kelembagaan Siber TNI AD

Dari perspektif *Ends,* penguatan struktur dan kelembagaan siber diarahkan untuk menjamin perlindungan sistem komando dan kendali sebagai pusat gravitasi modern kekuatan militer. Pembelajaran dari Ukraina menunjukkan bahwa negara yang memiliki struktur komando siber yang jelas dan terpusat mampu mempertahankan keberlangsungan operasi meskipun berada di bawah tekanan serangan siber yang intensif. Pada aspek *Ways*, penguatan kelembagaan dilakukan melalui penegasan peran Pussansiad sebagai koordinator utama pertahanan siber TNI AD, serta integrasi fungsi siber ke dalam sistem operasi militer. Pendekatan ini menuntut kejelasan hubungan komando, alur koordinasi, dan mekanisme respons insiden yang terstruktur dari pusat hingga satuan wilayah. Sedangkan, dari sisi *Means*, strategi ini membutuhkan validasi organisasi yang menyeluruh, pengisian struktur dengan personel siber yang memadai, serta dukungan anggaran dan perangkat pendukung yang berkelanjutan. Tanpa pemenuhan sumber daya yang seimbang, penguatan kelembagaan berisiko bersifat simbolik dan belum mampu memberikan dampak operasional yang signifikan.

b. Penguatan SDM Siber Profesional

Dalam kerangka *Ends*, penguatan SDM siber bertujuan memastikan tersedianya personel profesional yang mampu menjaga ketahanan sistem informasi dan mendukung

kesinambungan operasi militer. Perang Rusia–Ukraina menunjukkan bahwa keunggulan siber sangat ditentukan oleh kualitas operator dan analis, bukan semata oleh teknologi. Pada aspek *Ways*, peningkatan profesionalisme SDM dilakukan melalui pendidikan berjenjang, pelatihan teknis lanjutan, sertifikasi siber, serta penugasan yang berkesinambungan pada fungsi-fungsi kritis. Pendekatan ini memungkinkan terbentuknya kompetensi yang adaptif terhadap perubahan taktik dan teknik serangan siber. Sedangkan sisi *Means*, strategi ini menuntut ketersediaan jumlah personel yang memadai, pola pembinaan karier siber yang jelas, serta insentif yang mendukung keberlanjutan SDM. Tanpa dukungan tersebut, kapasitas SDM siber akan sulit berkembang dan tidak mampu mengimbangi eskalasi ancaman siber modern.

c. Modernisasi Infrastruktur Siber dan Integrasi C5ISR

Tujuan strategis (*Ends*) dari modernisasi infrastruktur siber adalah memastikan keandalan sistem informasi dan integrasi siber dalam sistem C5ISR guna mendukung pengambilan keputusan dan efektivitas operasi militer. Konflik Rusia–Ukraina memperlihatkan bahwa kegagalan melindungi sistem ini berdampak langsung pada menurunnya efektivitas operasi lapangan. Pada tataran ***Ways***, modernisasi dilakukan melalui penguatan sistem pemantauan, deteksi dini, respons insiden, serta integrasi data siber dengan fungsi intelijen, pengawasan, dan pengintaian. Pendekatan ini memungkinkan respons yang lebih cepat dan terkoordinasi terhadap ancaman yang bersifat multivektor. Adapun pada aspek *Means*, strategi ini memerlukan pemerataan perangkat keamanan, peningkatan kapasitas sistem, serta integrasi teknologi antar satuan. Keterbatasan infrastruktur dan fragmentasi sistem akan melemahkan efektivitas integrasi C5ISR dan mengurangi daya tangkal pertahanan siber secara keseluruhan.

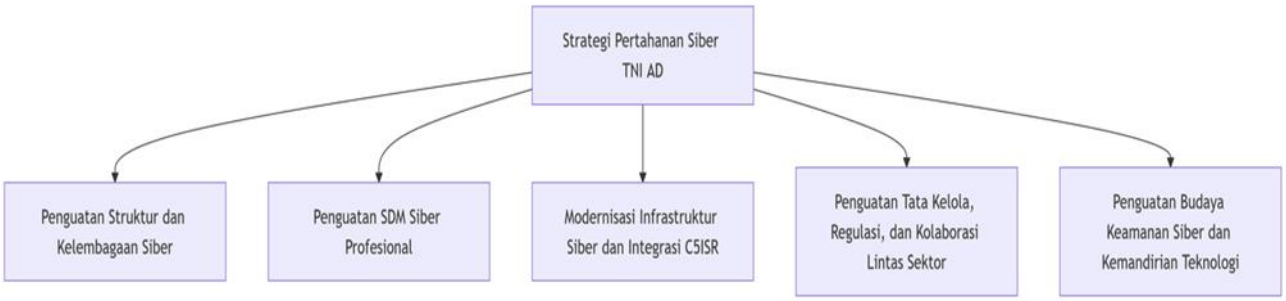
d. Penguatan Tata Kelola, Regulasi, dan Kolaborasi Lintas Sektor

Dalam perspektif *Ends*, tata kelola dan regulasi bertujuan menciptakan kepastian hukum dan kerangka kerja yang mendukung penyelenggaraan pertahanan siber secara konsisten dan terkoordinasi. Pembelajaran dari Ukraina menunjukkan bahwa koordinasi lintas lembaga menjadi faktor penting dalam menghadapi serangan siber skala nasional. Pada aspek *Ways*, penguatan dilakukan melalui penyelarasan regulasi internal TNI AD dengan kebijakan nasional, serta pengembangan mekanisme kerja sama lintas sektor, termasuk dengan kementerian, lembaga, dan mitra strategis lainnya. Pendekatan ini memungkinkan respons kolektif terhadap ancaman siber yang bersifat lintas domain. Sedangkam dari sisi *Means*, implementasi tata kelola memerlukan kapasitas kelembagaan, sumber daya hukum, serta sistem koordinasi yang efektif, tanpa dukungan tersebut, regulasi berpotensi hanya bersifat normatif dan belum sepenuhnya berdampak pada praktik operasional.

e. Penguatan Budaya Keamanan Siber dan Kemandirian Teknologi

Tujuan strategis (*Ends*) dari penguatan budaya keamanan siber adalah membangun kesadaran kolektif bahwa keamanan siber merupakan tanggung jawab seluruh personel, bukan hanya unit teknis. Perang Rusia–Ukraina menunjukkan bahwa kelalaian individu dapat menjadi pintu masuk serangan siber yang berdampak luas. Pada aspek *Ways*, budaya keamanan dibangun melalui internalisasi nilai keamanan informasi, disiplin penggunaan sistem digital, serta peningkatan literasi siber di seluruh jajaran. Upaya ini diperkuat dengan langkah menuju kemandirian teknologi guna mengurangi risiko ketergantungan pada perangkat asing. Dari sisi *Means*, strategi ini membutuhkan dukungan kebijakan, program edukasi berkelanjutan, serta pengembangan dan pemanfaatan teknologi dalam negeri. Tanpa penguatan sumber daya ini, budaya keamanan siber sulit tumbuh secara konsisten dan berkelanjutan.

Dapat disimpulkan bahwa strategi pertahanan siber TNI AD berdasarkan pembelajaran perang Rusia–Ukraina menegaskan bahwa keberhasilan pertahanan siber sangat bergantung pada keseimbangan antara ends, ways, dan means. Penguatan pada satu unsur tanpa diikuti unsur lainnya berpotensi melemahkan efektivitas strategi. Oleh karena itu, TNI AD perlu membangun strategi pertahanan siber yang terintegrasi, berkelanjutan, dan adaptif agar mampu menghadapi ancaman siber modern yang semakin kompleks dan terkoordinasi. Untuk memudahkan pemahaman panalisis pembahasan di atas, berikut di bawah ini gambar dan tabel pemetaan strategi pertahanan TNI AD dalam menghadapi ancaman siber berdasarkan perang Rusia-Ukraina periode 2013-2024, menurut kerangka *Ends, Ways, Means.*



Gambar 5. Strategi pertahanan TNI AD dalam menghadapi ancaman siber berdasarkan Perang Rusia-Ukraina periode 2014-2023
Sumber : data diolah peneliti (2025)

Tabel 4. Pemetaan Komponen Strategi pada Kerangka *Ends, Ways, Means*

No.	Komponen Strategi	Kerangka *Ends, Ways, Means*	Data temuan di lapangan
1	**2**	**3**	**4**
1.	Penguatan Struktur dan Kelembagaan Siber TNI AD	*Ends*	Struktur siber sudah berjalan, namun belum merata dan masih memerlukan konsolidasi lintas matra dan lembaga.
2.	Penguatan SDM Siber Profesional	*Means*	SDM memiliki kompetensi dasar, namun jumlah tenaga ahli dan personel tersertifikasi masih terbatas.
3.	Modernisasi Infrastruktur Siber dan Integrasi C5ISR	*Ways*	Infrastruktur & sistem teknologi siber sudah ad namun distribusi perangkat dan sensor ancaman belum merata di Kotama/Balakpus.
4.	Penguatan Tata Kelola, Regulasi, dan Kolaborasi Lintas Sektor	*Ways*	SOP dan regulasi sudah ada, namun implementasinya belum konsisten dan koordinasi lintas lembaga belum optimal
5.	Penguatan Budaya Keamanan Siber dan Kemandirian Teknologi	*Ways*	Kesadaran keamanan masih rendah dan ketergantungan perangkat asing meningkatkan kerentanan.

Sumber : data diolah peneliti (2025)

KESIMPULAN

Penelitian ini menyimpulkan bahwa kesiapan pertahanan siber TNI AD berada pada tahap berkembang. TNI AD telah memiliki fondasi kelembagaan, regulasi dasar, SDM awal, dan infrastruktur pendukung, namun pemerataan kapasitas, integrasi operasional, dan konsistensi implementasi masih memerlukan penguatan. Pembangunan strategi pertahanan siber dipengaruhi oleh interaksi faktor internal dan eksternal. Faktor internal menyediakan

kerangka kelembagaan dan kebijakan, sementara faktor eksternal menghadirkan peluang sekaligus tantangan melalui eskalasi ancaman siber dan dinamika geopolitik. Pembelajaran dari perang Rusia–Ukraina menegaskan bahwa siber merupakan bagian integral dari operasi militer modern, sehingga strategi pertahanan siber TNI AD perlu dibangun secara terintegrasi antara tujuan strategis, pendekatan operasional, dan kapasitas sumber daya.

Saran

Secara teoritis, penelitian ini merekomendasikan penguatan kerangka analisis strategi pertahanan siber berbasis *Ends–Ways–Means* sebagai alat untuk menilai keselarasan antara tujuan strategis, pendekatan operasional, dan kapasitas sumber daya. Secara praktis, TNI AD bersama pemangku kepentingan terkait perlu memperkuat pemerataan kapasitas siber, profesionalisme SDM, integrasi sistem C5ISR, tata kelola yang adaptif, serta budaya keamanan dan kemandirian teknologi guna meningkatkan ketahanan siber institusi secara berkelanjutan.

DAFTAR PUSTAKA

Amalia, A. F., & Atman, W. (2025). Strategi deterrence siber Indonesia terhadap ancaman proxy state actor. *Jurnal Pertahanan dan Bela Negara, 15*(1), 262–277.

Anjelina, D. (2023). Fenomena serangan siber Rusia terhadap Ukraina sebagai pembelajaran bagi Indonesia dalam pengembangan pertahanan siber. *Jurnal Pertahanan dan Bela Negara, 13*(3), 231–241.

Arreguín-Toft, I. (2001). How the weak win wars: A theory of asymmetric conflict. *International Security, 26*(1), 93–128. https://doi.org/10.1162/016228801753212868

Bakrie, R. C., et al. (2022). The influence of the Russian and Ukrainian wars on the economy of Southeast Asia. *Caraka Prabu: Jurnal Ilmu Pemerintahan, 6*(1), 65–86.

Budiman, D. W., et al. (2023). *Perang Rusia–Ukraina dalam perspektif siber: Sebuah literasi*. Politeknik Siber dan Sandi Negara Press.

Budiman, I., et al. (2023). Cybersecurity analysis in the context of the Russia–Ukraine conflict. *Jurnal Ekonomi, 12*(2), 50–65.

Clausewitz, C. v. (1984). *On war* (M. Howard & P. Paret, Trans.). Princeton University Press. (Original work published 1832)

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Erickson, J. V. (2021). Clausewitz's perspective on deterring Russian malign activities in cyberspace. *Military Review*, September–October, 6–11.

Gray, C. S. (2010). *The strategy bridge: Theory for practice*. Oxford University Press.

Imma, K., & Burhanuddin, A. (2023). Signifikansi perang siber dalam konflik modern Rusia–Ukraina. *JISHUM: Jurnal Ilmu Sosial dan Humaniora, 1*(4), 800–817. https://doi.org/10.57248/jishum.v1i4.155

Itzhak, A., & Ferri, U. (2023). Russian–Ukraine armed conflict: Lessons learned on the digital ecosystem. *International Journal of Critical Infrastructure Protection, 43*, 100637. https://doi.org/10.1016/j.ijcip.2023.100637

Khoirunnisa, K., & Sugiati, C. (2024). Cyber warfare strategies in the Russia–Ukraine conflict (2021–2022). *Jurnal Public Policy, 10*(2), 138–150. https://doi.org/10.35308/jpp.v10i2.9026

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE Publications.

Miron, M., & Thornton, R. (2024). The use of cyber tools by the Russian military: Lessons from the war against Ukraine. *Applied Cybersecurity and Internet Governance, 3*(1), 147–169.

https://doi.org/10.60097/ACIG/190142
Nye, J. S., Jr. (2011). Power and national security in cyberspace. In K. M. Lord & T. Sharp (Eds.), *America's cyber future: Security and prosperity in the information age* (Vol. II, pp. 5–23). Center for a New American Security.
Rid, T. (2012). Cyber war will not take place. *The Journal of Strategic Studies, 35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939
Sarjito, A. (2024). Formation of the TNI cyber force: A strategic and policy analysis. *Defense and Security Studies, 5*(2), 74–83. https://doi.org/10.37868/dss.v5.id272
Sugiyono. (2018). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.
Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security* (6th ed.). Cengage Learning.
Widjajanto, A. (2020). Strategi pertahanan negara dalam menghadapi ancaman non-tradisional. *Jurnal Pertahanan*.
World Economic Forum. (2023). *Global cybersecurity outlook 2023*. https://www.weforum.org