



Analisis Perang Kontemporer dan Implikasinya terhadap Pembangunan Kekuatan Tentara Nasional Indonesia (TNI)

*Analysis of Contemporary Warfare and Its Implications for the Development of the
Indonesian National Armed Forces (TNI)*

Irwan Achiranto

(APN Ahli Madya Renhan Kemhan)

irwanachirianto@gmail.com

Abstract

Contemporary warfare has undergone profound transformations that have reshaped global paradigms of national security and defense. Conflicts are no longer confined to conventional state-to-state confrontations but increasingly involve non-state actors, disruptive technologies, and new domains such as cyberspace and outer space. In this context, the Indonesian National Armed Forces (TNI) face strategic challenges in adapting their posture, doctrine, and military capabilities to remain relevant amid the evolving nature of modern threats. This article critically analyzes the transformation of contemporary warfare and its implications for the direction of TNI's force development. A qualitative-descriptive approach is employed, drawing on literature analysis of national defense policies, military doctrines, and strategic reports from international defense and security institutions. The findings indicate that the transformation of warfare toward multidomain operations—including hybrid, cyber, and information warfare—demands comprehensive modernization of weapon systems, enhanced interoperability among service branches, and reform of military doctrine and education. The development of TNI's strength should focus on the integration of advanced technologies, the strengthening of digital capacities, and cross-sectoral synergy within a whole-of-government framework. Consequently, TNI must evolve into an adaptive, responsive, and sustainable defense force capable of addressing the increasingly complex spectrum of threats in the 21st century.

Keywords: *contemporary warfare, Indonesian National Armed Forces (TNI), national defense, hybrid warfare, cyber security*

Abstrak

Perang kontemporer telah mengalami transformasi mendalam yang mengubah paradigma keamanan dan pertahanan negara di seluruh dunia. Konflik tidak lagi hanya terjadi dalam bentuk konvensional antar negara, tetapi melibatkan aktor non-

negara, teknologi disruptif, serta domain baru seperti siber dan ruang angkasa. Dalam konteks ini, Tentara Nasional Indonesia (TNI) dihadapkan pada tantangan strategis untuk menyesuaikan postur, doktrin, dan kapabilitas militernya agar tetap relevan dengan karakteristik ancaman modern. Artikel ini bertujuan untuk menganalisis secara kritis perubahan karakter perang kontemporer serta implikasinya terhadap arah pembangunan kekuatan TNI. Pendekatan penelitian bersifat kualitatif-deskriptif dengan analisis literatur terhadap kebijakan pertahanan nasional, doktrin militer, serta laporan strategis lembaga pertahanan dan keamanan internasional. Hasil analisis menunjukkan bahwa transformasi perang ke arah multidomain—yang mencakup perang hibrida, siber, dan informasi—menuntut pembaruan menyeluruh dalam modernisasi alutsista, peningkatan interoperabilitas antar matra, serta reformasi doktrin dan pendidikan militer. Pembangunan kekuatan TNI harus diarahkan pada integrasi teknologi tinggi, penguatan kapasitas digital, dan sinergi lintas sektor dalam kerangka pendekatan *whole-of-government*. Dengan demikian, TNI dituntut menjadi kekuatan pertahanan yang adaptif, responsif, dan berkelanjutan dalam menghadapi spektrum ancaman yang semakin kompleks di abad ke-21.

Kata kunci: perang kontemporer, TNI, pertahanan nasional, perang hibrida, keamanan siber

Pendahuluan

Perang sebagai fenomena politik dan sosial selalu berevolusi mengikuti dinamika peradaban manusia. Sejak era Clausewitz, perang dipahami sebagai kelanjutan politik dengan cara lain, namun pada abad ke-21, definisi ini menghadapi tantangan baru. Globalisasi, kemajuan teknologi, dan interdependensi ekonomi telah mengubah wajah konflik dari konfrontasi terbuka menjadi persaingan multidimensi yang bersifat asimetris dan tidak terprediksi (Kaldor, 2013; Walzer, 2015). Dalam lanskap geopolitik kontemporer, perang tidak lagi berlangsung semata-mata antarnegara berdaulat, tetapi melibatkan aktor non-negara, kelompok transnasional, dan entitas digital yang beroperasi di ruang siber tanpa batas geografis.

Transformasi karakter perang ini terlihat dalam munculnya bentuk-bentuk seperti *hybrid warfare*, *cyber warfare*, dan *information operations* yang telah menjadi bagian integral dari strategi militer modern (Hoffman, 2007). Perang hibrida, misalnya, menggabungkan kekuatan militer tradisional dengan taktik non-militer

seperti disinformasi, tekanan ekonomi, dan infiltrasi politik. Di sisi lain, perang siber dan operasi informasi memungkinkan negara atau aktor non-negara melumpuhkan sistem pertahanan lawan tanpa perlu konfrontasi fisik. Fenomena ini memperluas definisi perang ke arah yang multidomain, di mana pertempuran berlangsung secara simultan di darat, laut, udara, ruang angkasa, dan siber (Gray, 2010).

Bagi Indonesia, perubahan karakter perang memiliki implikasi strategis yang signifikan terhadap kebijakan pertahanan nasional dan arah pembangunan kekuatan TNI. Sebagai komponen utama pertahanan negara, TNI memiliki tanggung jawab untuk menjaga kedaulatan, keutuhan wilayah, dan keselamatan bangsa dari segala bentuk ancaman. Namun, sistem pertahanan yang masih berorientasi pada model konvensional menghadapi tantangan besar dalam menyesuaikan diri dengan sifat konflik modern yang berbasis teknologi dan informasi (Siregar, 2021). Keteringgalan dalam penguasaan teknologi digital, keterbatasan interoperabilitas antar matra, serta doktrin yang belum sepenuhnya mencerminkan dinamika ancaman multidomain menjadi isu krusial yang harus segera diatasi.

Pembangunan kekuatan TNI tidak dapat dilepaskan dari dinamika global dan regional yang terus berubah. Rivalitas strategis antara kekuatan besar seperti Amerika Serikat, Tiongkok, dan Rusia telah mempercepat perlombaan persenjataan canggih, termasuk dalam bidang kecerdasan buatan, drone otonom, dan sistem pertahanan siber (Bitzinger, 2020). Sementara itu, di kawasan Indo-Pasifik, kompetisi geopolitik semakin mengemuka, terutama dalam konteks Laut Cina Selatan yang menjadi arena kontestasi strategis. Dalam konteks ini, posisi Indonesia sebagai negara kepulauan dengan wilayah strategis menuntut kesiapan TNI yang mampu beroperasi secara efektif dalam berbagai domain dan skenario ancaman.

Selain faktor eksternal, faktor internal seperti keterbatasan anggaran pertahanan, modernisasi alutsista yang berjalan lambat, dan kebutuhan reformasi kelembagaan juga menjadi tantangan utama. Data Renstra Kementerian Pertahanan (Kemhan RI, 2020) menunjukkan bahwa sebagian besar platform utama TNI masih

mengandalkan sistem lama, sementara integrasi teknologi berbasis kecerdasan buatan, analisis data besar (*big data*), dan *command and control system* berbasis digital belum sepenuhnya terwujud. Di tengah transformasi global menuju perang berbasis teknologi, kesenjangan ini dapat menurunkan daya tangkal dan efektivitas operasional pertahanan nasional.

Di sisi lain, munculnya ancaman non-tradisional seperti terorisme, ekstremisme, dan kejahatan siber menambah kompleksitas lingkungan strategis Indonesia. Aktor non-negara kini mampu mengganggu stabilitas nasional melalui taktik murah namun efektif seperti propaganda digital, sabotase infrastruktur, dan infiltrasi informasi publik (Ridwan, 2022). Dalam konteks ini, TNI tidak dapat mengandalkan pendekatan militer semata, tetapi harus mengintegrasikan strategi multidimensi yang melibatkan kerja sama lintas lembaga dan sektor sipil, sesuai dengan prinsip *whole-of-government approach*.

Melihat kondisi tersebut, analisis terhadap karakteristik perang kontemporer dan implikasinya terhadap pembangunan kekuatan TNI menjadi urgensi strategis. Pemahaman terhadap transformasi ini akan menentukan efektivitas kebijakan pertahanan nasional dalam menghadapi ancaman masa depan. Tulisan ini berupaya mengisi kesenjangan analitis dengan menjawab pertanyaan: bagaimana perang kontemporer membentuk arah pembangunan kekuatan TNI, dan langkah-langkah apa yang perlu dilakukan agar TNI tetap relevan di era konflik multidomain?

Tujuan utama artikel ini adalah untuk menganalisis secara sistematis pengaruh perang kontemporer terhadap strategi, doktrin, dan struktur kekuatan TNI. Melalui kajian literatur, analisis kebijakan, dan sintesis terhadap doktrin militer modern, tulisan ini diharapkan memberikan kontribusi terhadap perumusan kebijakan pertahanan yang adaptif, inovatif, dan berkelanjutan. Secara akademik, penelitian ini juga memperkaya kajian ilmu pertahanan dengan menawarkan perspektif multidomain dalam konteks Indonesia, sekaligus menegaskan pentingnya modernisasi pertahanan dalam menghadapi tantangan abad ke-21.

Tinjauan Pustaka dan Kerangka Teori

1. Evolusi Teori Perang dalam Perspektif Kontemporer

Kajian mengenai perang dan strategi militer telah mengalami perubahan mendasar seiring dengan berkembangnya konteks geopolitik dan teknologi global. Klasikisme Clausewitz yang menyatakan bahwa “perang adalah kelanjutan politik dengan cara lain” (Clausewitz, 1976) menjadi fondasi teori tradisional yang menekankan aspek kekuasaan, militer konvensional, dan kemenangan fisik di medan perang. Namun, paradigma tersebut mulai tergeser sejak akhir abad ke-20 ketika konflik internasional menampilkan kompleksitas baru berupa keterlibatan aktor non-negara, medan tempur non-fisik, dan instrumen perang berbasis informasi.

Mary Kaldor (2013) memperkenalkan konsep *new wars* yang menandai pergeseran dari perang antarnegara ke perang intra-negara dengan karakter etno-politik, ekonomi ilegal, dan partisipasi non-negara. Dalam konteks modern, perang menjadi campuran antara militerisme dan politik identitas yang diperkuat oleh teknologi digital dan globalisasi informasi. Sementara itu, Martin van Creveld (2008) menyebut fenomena ini sebagai *transformation of war*, yaitu pergeseran dari perang industri ke perang post-modern yang lebih desentralistik, fleksibel, dan berbasis jaringan.

Perang kontemporer tidak lagi menitikberatkan pada kemenangan teritorial, melainkan pada dominasi persepsi dan kontrol informasi (Arquilla & Ronfeldt, 1997). Artinya, kekuatan militer yang efektif tidak hanya bergantung pada alutsista dan jumlah pasukan, tetapi juga pada kemampuan negara dalam mengelola *cyber power*, *information superiority*, serta kapasitas intelijen digital. Dalam kerangka inilah muncul konsep *hybrid warfare*, yang pertama kali diperkenalkan oleh Frank Hoffman (2007) untuk menjelaskan kombinasi antara operasi militer konvensional, taktik irreguler, perang siber, dan propaganda informasi sebagai satu kesatuan strategi.

2. Perang Multidomain dan Teknologi Pertahanan

Transformasi teknologi militer menjadi katalis utama perubahan karakter perang modern. Konsep *multi-domain operations (MDO)* yang dikembangkan oleh militer Amerika Serikat menegaskan pentingnya integrasi antara domain darat, laut, udara, ruang angkasa, dan siber (U.S. Army Training and Doctrine Command, 2018). Dalam kerangka ini, keunggulan strategi militer ditentukan oleh kemampuan integratif lintas domain melalui pemanfaatan kecerdasan buatan (*artificial intelligence/AI*), sistem otonom, dan *network-centric warfare* (Alkire et al., 2020).

Teknologi *drone swarm*, sensor presisi tinggi, serta sistem *command and control* berbasis AI mengubah pola operasi menjadi lebih cepat, presisi, dan minim risiko personel. Menurut Singer (2010), otomatisasi perang menandai era “robotics revolution” di mana keputusan tempur tidak lagi hanya diambil manusia, tetapi juga oleh algoritma. Fenomena ini menimbulkan implikasi etis dan strategis, termasuk pada kapasitas adaptasi militer nasional terhadap percepatan teknologi global.

Dalam konteks Indonesia, ketertinggalan teknologi pertahanan menjadi tantangan utama bagi TNI. Data dari Kementerian Pertahanan (Kemhan RI, 2020) menunjukkan bahwa modernisasi sistem senjata strategis (*MEF—Minimum Essential Force*) masih menghadapi kendala dalam pendanaan, industri pertahanan nasional, serta integrasi teknologi digital. Sementara itu, doktrin militer Indonesia masih berorientasi pada strategi pertahanan teritorial yang bersifat defensif dan konvensional. Padahal, di era perang multidomain, strategi semacam ini perlu dilengkapi dengan kemampuan ofensif di ruang siber, informasi, dan kognitif.

3. Kerangka Teori: Pendekatan Multidomain dan Strategi Adaptif

Kerangka teori yang digunakan dalam penelitian ini menggabungkan dua perspektif utama, yaitu teori *multidomain warfare* dan konsep *adaptive military transformation*.

Pertama, teori *multidomain warfare* menjelaskan bahwa keberhasilan operasi militer bergantung pada integrasi lintas domain, di mana setiap elemen kekuatan (darat, laut, udara, siber, dan ruang angkasa) berfungsi secara sinergis untuk

mencapai efek strategis tunggal (Gray, 2010). Pendekatan ini menekankan bahwa perang tidak lagi linear, tetapi simultan dan saling terkait dalam ruang fisik dan non-fisik.

Kedua, konsep *adaptive military transformation* (Farrell & Terriff, 2002) menjelaskan bahwa efektivitas militer di era modern bergantung pada kemampuan institusi pertahanan beradaptasi terhadap perubahan lingkungan strategis. Transformasi adaptif meliputi tiga dimensi utama: (1) **transformasi doktrinal**, yaitu pembaruan paradigma dan strategi pertahanan; (2) **transformasi kelembagaan**, berupa reorganisasi struktur dan mekanisme komando; serta (3) **transformasi teknologi**, yaitu modernisasi sistem senjata dan integrasi sistem informasi pertahanan.

Dalam konteks TNI, kedua pendekatan ini memberikan landasan teoretis untuk memahami bagaimana perubahan karakter perang memengaruhi arah pembangunan kekuatan militer nasional. TNI dituntut untuk bertransformasi tidak hanya dalam aspek teknologi, tetapi juga dalam dimensi organisasi, budaya militer, dan pola pikir strategis. Sebagaimana ditegaskan oleh Dibb dan Brabin-Smith (2021), keberhasilan transformasi pertahanan nasional di abad ke-21 tidak hanya ditentukan oleh kemampuan berperang, tetapi juga oleh kemampuan beradaptasi terhadap perubahan.

4. Relevansi terhadap Pembangunan Kekuatan TNI

Secara empiris, TNI berada pada titik kritis untuk menyeimbangkan antara warisan strategi konvensional dan kebutuhan transformasi modern. Doktrin pertahanan Indonesia yang menekankan *total defense system* (sistem pertahanan semesta) memiliki keunggulan dalam aspek mobilisasi rakyat dan ketahanan sosial, namun masih terbatas dalam menjawab ancaman digital dan non-konvensional (Kemhan RI, 2020).

Kajian Lembaga Ketahanan Nasional (Lemhannas, 2022) menegaskan pentingnya penguatan *cyber defense command*, *information warfare division*, dan *rapid response task force* untuk mempercepat kesiapsiagaan nasional terhadap ancaman multidomain. Dengan kata lain, pembangunan kekuatan TNI perlu bergeser dari paradigma kuantitatif menuju paradigma kualitatif—yang menekankan kecepatan, kecerdasan, interoperabilitas, dan adaptivitas.

Selain itu, penerapan konsep *whole-of-government approach* menjadi kunci sinergi antara TNI, Kemhan, BSSN, BIN, dan Kemenkominfo. Sinergi ini memungkinkan pertahanan nasional beroperasi dalam satu ekosistem keamanan yang terintegrasi (Nugraha, 2023).

Kerangka teori di atas menjadi fondasi bagi analisis berikutnya yang membahas bagaimana perang kontemporer—melalui perang hibrida, dominasi teknologi, dan ancaman non-tradisional—secara langsung membentuk arah pembangunan kekuatan TNI dari sisi doktrin, struktur, SDM, dan teknologi.

Metode Penelitian

Penelitian ini menggunakan pendekatan **kualitatif-deskriptif** yang bertujuan memahami dan menjelaskan secara mendalam fenomena perubahan karakter perang kontemporer serta implikasinya terhadap strategi pembangunan kekuatan Tentara Nasional Indonesia (TNI). Pendekatan ini dipilih karena permasalahan yang dikaji bersifat konseptual, strategis, dan multidimensional, sehingga tidak dapat dijelaskan secara memadai melalui metode kuantitatif. Penelitian ini bersifat **analitis dan eksploratif**, menggabungkan kajian teoritis dengan analisis kebijakan pertahanan nasional. Fokus utamanya bukan untuk menguji hipotesis, tetapi untuk membangun pemahaman baru serta merumuskan rekomendasi strategis yang relevan bagi penguatan postur TNI dalam menghadapi tantangan perang multidomain.

Proses penelitian dilakukan melalui interpretasi mendalam terhadap dokumen resmi, literatur akademik, dan data kebijakan yang relevan. Mengacu pada

pandangan Creswell dan Creswell (2018), pendekatan kualitatif memungkinkan peneliti menafsirkan realitas sosial dan politik secara kontekstual, terutama dalam isu strategis dan kebijakan publik. Dalam penelitian ini, metode tersebut diterapkan untuk mengidentifikasi pola transformasi perang modern dan menilai sejauh mana TNI beradaptasi terhadap dinamika lingkungan strategis global dan regional.

Data penelitian diperoleh dari berbagai sumber primer dan sekunder. Sumber primer meliputi dokumen resmi pemerintah seperti *Rencana Strategis Kementerian Pertahanan 2020–2024*, *Doktrin TNI* untuk ketiga matra (AD, AL, dan AU), serta *Strategi Keamanan Siber Nasional* yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN). Sementara itu, sumber sekunder terdiri atas literatur akademik dan laporan lembaga internasional, termasuk publikasi dari *United Nations Office for Disarmament Affairs (UNODA)*, *NATO Defense College*, dan berbagai jurnal ilmiah yang membahas *hybrid warfare*, *multi-domain operations*, serta transformasi pertahanan (*defense transformation*). Kajian empiris juga didukung oleh hasil penelitian lembaga nasional seperti Lembaga Ketahanan Nasional (Lemhannas), Pusat Penelitian dan Pengembangan Strategi TNI (Pusjianstralitbang TNI), dan Kementerian Riset dan Teknologi/BRIN yang berfokus pada inovasi pertahanan. Seluruh data dikumpulkan melalui teknik **studi pustaka** (*library research*) dengan pengelompokan tematik yang mencakup karakteristik perang kontemporer, arah modernisasi TNI, dan kebijakan pertahanan nasional.

Tahapan analisis dilakukan secara **interpretatif-kualitatif** dengan tiga langkah utama: reduksi data, kategorisasi tematik, dan sintesis argumentatif (Miles, Huberman, & Saldaña, 2014). Pertama, data yang dikumpulkan dari dokumen dan literatur diidentifikasi berdasarkan relevansinya terhadap isu strategis yang sedang diteliti. Kedua, data dikategorikan menurut empat dimensi utama: doktrin, teknologi, organisasi, dan sumber daya manusia. Ketiga, dilakukan sintesis terhadap hubungan antarvariabel tersebut untuk membangun kerangka analisis mengenai bagaimana perubahan karakter perang memengaruhi arah pembangunan kekuatan TNI. Dalam tahap ini digunakan pula **analisis isi** (*content analysis*) guna menelusuri makna

eksplisit dan implisit dari kebijakan pertahanan, serta **analisis wacana** (*discourse analysis*) untuk memahami bagaimana isu perang modern dibingkai dalam konteks politik dan kebijakan pertahanan nasional. Sejalan dengan pemikiran Krippendorff (2018), metode analisis isi dipandang efektif untuk mengungkap struktur makna dan ideologi yang tersembunyi di balik teks strategis dan dokumen kebijakan.

Validitas dan kredibilitas data dijamin melalui **triangulasi sumber dan metode**. Perbandingan dilakukan antara data resmi pemerintah, publikasi akademik, dan hasil penelitian independen untuk memastikan konsistensi temuan. Proses validasi juga melibatkan *peer review* oleh pakar strategi pertahanan dan akademisi di bidang ilmu militer guna memperkuat reliabilitas analisis. Pendekatan multiperspektif ini penting agar hasil penelitian tidak hanya bersifat konseptual, tetapi juga dapat diaplikasikan dalam kerangka kebijakan pertahanan nasional.

Ruang lingkup penelitian dibatasi pada periode 2010–2025, yaitu fase ketika transformasi digital dan konsep perang multidomain berkembang pesat di tingkat global. Rentang waktu ini relevan untuk menilai adaptasi TNI terhadap perubahan paradigma konflik yang melibatkan domain fisik dan non-fisik secara bersamaan. Penelitian tidak mencakup observasi lapangan atau survei militer, karena fokus utamanya adalah pada analisis konseptual dan kebijakan strategis, bukan pada aspek operasional atau taktis. Dengan demikian, hasil penelitian ini bersifat normatif-analitis dan ditujukan untuk mendukung proses pengambilan keputusan di tingkat strategis.

Dengan desain metodologis semacam ini, penelitian diharapkan mampu memberikan pemahaman komprehensif mengenai hubungan antara dinamika perang kontemporer dan arah pembangunan kekuatan TNI. Selain itu, pendekatan ini memperkuat dasar konseptual bagi transformasi pertahanan Indonesia menuju kekuatan yang adaptif, inovatif, dan berdaya saing di tingkat global—suatu prasyarat mutlak dalam menghadapi kompleksitas konflik dan ancaman hibrida di abad ke-21.

Analisis dan Pembahasan

1. Transformasi Karakter Perang di Era Kontemporer

Perang kontemporer menunjukkan dinamika yang berbeda secara fundamental dari bentuk konflik tradisional yang berfokus pada konfrontasi militer antarnegara. Dalam konteks global, perang kini melibatkan dimensi politik, ekonomi, teknologi, dan sosial secara simultan, yang dikenal sebagai *multidimensional conflict environment* (Freedman, 2017). Pergeseran ini tidak hanya memengaruhi cara negara mempertahankan diri, tetapi juga mengubah makna kekuatan militer itu sendiri.

Salah satu ciri utama perang kontemporer adalah munculnya **perang hibrida (hybrid warfare)**—strategi yang menggabungkan operasi militer konvensional dengan taktik non-konvensional seperti propaganda digital, disinformasi, tekanan ekonomi, dan serangan siber (Hoffman, 2007). Perang Rusia–Ukraina merupakan contoh paling jelas dari model ini, di mana kekuatan militer dikombinasikan dengan operasi psikologis, propaganda, dan serangan siber terhadap infrastruktur penting (Galeotti, 2022). Bentuk perang semacam ini memperlihatkan bahwa kemenangan tidak lagi hanya diukur melalui penguasaan wilayah, tetapi juga melalui dominasi persepsi dan kontrol informasi publik.

Selain itu, perang modern ditandai oleh **penggunaan teknologi disruptif** seperti kecerdasan buatan (*artificial intelligence*), sistem senjata otonom, dan drone swarm. Penguasaan teknologi ini memungkinkan serangan presisi tinggi dengan risiko minimal terhadap personel, sekaligus memperluas ruang tempur ke domain baru: **siber dan ruang angkasa** (Singer, 2010; Bitzinger, 2020). Konsep *multi-domain operations (MDO)* menggarisbawahi bahwa seluruh elemen kekuatan—darat, laut, udara, ruang angkasa, dan siber—harus terintegrasi secara real time dalam satu sistem komando dan kendali (TRADOC, 2018).

Perubahan ini juga berdampak pada struktur aktor dalam perang. Konflik tidak lagi terbatas pada entitas negara, melainkan melibatkan **aktor non-negara** seperti

kelompok teroris, milisi transnasional, dan bahkan korporasi digital yang memiliki kapasitas intelijen dan siber (Kaldor, 2013). Mereka menggunakan taktik asimetris yang bersifat murah, cepat, dan sulit dideteksi. Dalam konteks ini, ancaman terhadap kedaulatan negara dapat muncul tanpa deklarasi perang, tetapi melalui disrupsi digital, manipulasi opini publik, atau sabotase ekonomi.

Bagi Indonesia, transformasi ini menuntut redefinisi menyeluruh terhadap konsep ancaman dan strategi pertahanan nasional. TNI, sebagai tulang punggung pertahanan negara, harus mampu mengembangkan kapabilitas yang melampaui batas-batas konvensional dan siap menghadapi ancaman multidimensi yang bersifat simultan, lintas domain, dan non-linear (Kemhan RI, 2020).

2. Implikasi Strategis terhadap Postur dan Doktrin TNI

a. Modernisasi Alutsista dan Transformasi Teknologi

Modernisasi alutsista TNI merupakan salah satu prioritas utama dalam menghadapi dinamika perang kontemporer. Namun, proses ini masih menghadapi berbagai tantangan struktural dan fiskal. Berdasarkan *Renstra Pertahanan 2020–2024*, pencapaian *Minimum Essential Force (MEF)* baru mencapai sekitar 70% dari target, sementara sebagian besar platform utama masih mengandalkan teknologi lama (Kemhan RI, 2020).

Dalam konteks perang multidomain, modernisasi tidak dapat dipahami hanya sebagai penggantian peralatan militer, tetapi sebagai **integrasi sistem pertahanan berbasis jaringan (network-centric warfare)**. Sistem ini menuntut sinkronisasi antara sensor, komando, dan senjata melalui jaringan informasi digital. Dengan demikian, efisiensi dan ketepatan operasi militer dapat meningkat secara eksponensial.

Selain itu, **pengembangan teknologi otonom** seperti drone swarm dan sistem pengintaian berbasis AI dapat memperkuat kemampuan pengawasan maritim dan udara Indonesia. Hal ini sangat relevan dengan karakter geografis Indonesia sebagai negara kepulauan dengan wilayah pertahanan yang luas. Oleh karena itu, kolaborasi

antara TNI, industri pertahanan nasional, dan lembaga riset seperti BRIN perlu diperkuat agar pengembangan teknologi militer tidak sepenuhnya bergantung pada impor.

b. Reformasi Doktrin Pertahanan

Transformasi perang kontemporer menuntut pembaruan doktrin militer yang lebih fleksibel, adaptif, dan responsif terhadap perubahan lingkungan strategis. Doktrin lama yang berorientasi pada perang gerilya atau pertahanan teritorial perlu diperluas agar mencakup **skenario perang hibrida dan multidomain** (Pusjianstralitbang TNI, 2023).

Doktrin baru harus menekankan kemampuan integratif antara operasi konvensional dan non-konvensional, misalnya melalui *cyber operations*, *information warfare*, dan *psychological operations*. Seperti dikemukakan oleh Farrell dan Terriff (2002), keberhasilan militer modern sangat bergantung pada kemampuan institusi untuk beradaptasi terhadap lingkungan strategis baru melalui transformasi doktrin.

Dalam konteks ini, TNI **perlu mengembangkan konsep doktrin adaptif**, di mana keputusan operasional tidak hanya bersifat top-down, tetapi juga memungkinkan inovasi di tingkat lapangan melalui pemanfaatan data intelijen dan teknologi real-time. Pendekatan ini sesuai dengan model *mission command* yang diterapkan di banyak militer modern, yang menekankan fleksibilitas dan inisiatif taktis.

c. Penguatan Interoperabilitas antar Matra

Salah satu kelemahan mendasar TNI dalam konteks perang multidomain adalah masih terbatasnya interoperabilitas antara matra darat, laut, dan udara. Struktur komando yang hierarkis dan sektoral sering kali menghambat respons cepat terhadap ancaman lintas domain. Oleh karena itu, diperlukan penguatan **komando gabungan (joint command)** yang tidak hanya bersifat koordinatif tetapi juga operasional.

Pembentukan **Komando Gabungan Wilayah Pertahanan (Kogabwilhan)** merupakan langkah awal menuju sistem pertahanan integratif. Namun, agar lebih efektif, Kogabwilhan perlu dilengkapi dengan infrastruktur *real-time information sharing system* dan *digital decision-support platform*. Sistem semacam ini memungkinkan tiap matra beroperasi secara simultan dengan situational awareness yang sama—suatu prasyarat penting dalam perang multidomain (Gray, 2010).

3. Tantangan dan Peluang Transformasi Digital TNI

a. Ancaman Siber dan Operasi Informasi

Ruang siber kini menjadi domain baru dalam strategi militer modern. Serangan terhadap infrastruktur digital, sistem komunikasi, dan jaringan komando dapat melumpuhkan negara tanpa perlu konfrontasi fisik (BSSN, 2021). Dalam hal ini, Indonesia masih berada pada tahap awal penguatan pertahanan siber nasional.

Unit Cyber TNI telah dibentuk, tetapi kapasitasnya masih terbatas pada fungsi defensif. Di era *offensive cyber operations*, kemampuan pertahanan siber harus diperluas mencakup deteksi dini, kontra-infiltrasi, dan *counter-propaganda*. Seperti dikemukakan oleh Nye (2019), kekuatan siber bukan hanya kemampuan teknis, tetapi juga bentuk *soft power* yang dapat memengaruhi narasi global dan persepsi publik.

TNI perlu memperkuat kerja sama dengan **Badan Siber dan Sandi Negara (BSSN)**, **Badan Intelijen Negara (BIN)**, serta sektor swasta teknologi untuk membangun **ekosistem pertahanan siber nasional**. Selain itu, pengembangan kapasitas personel melalui pelatihan *cyber defense* dan *digital intelligence* menjadi bagian krusial dari strategi jangka panjang.

b. Pengelolaan Informasi dan Perang Kognitif

Perang kontemporer tidak hanya terjadi di ranah fisik dan digital, tetapi juga di ruang persepsi manusia—yang dikenal sebagai **perang kognitif (cognitive warfare)**.

Dalam skenario ini, tujuan utama bukan penghancuran fisik, melainkan manipulasi opini publik dan disorientasi psikologis masyarakat.

Menurut Lanoszka (2016), perang kognitif beroperasi dengan memanfaatkan algoritma media sosial, *deepfake*, dan propaganda digital untuk mengikis kepercayaan publik terhadap institusi negara. Di Indonesia, potensi ancaman semacam ini cukup tinggi, mengingat tingkat penetrasi media digital dan kerentanan terhadap disinformasi.

Untuk mengantisipasi hal ini, TNI harus mengembangkan **unit operasi informasi (Information Warfare Division)** yang berfungsi melakukan kontra-narasi, analisis psikologis, dan *strategic communication*. Unit ini akan berperan strategis dalam menjaga integritas informasi publik dan mendukung stabilitas sosial nasional di tengah dinamika proxy war.

c. Restrukturisasi Organisasi dan Inovasi SDM

Transformasi perang juga menuntut perubahan struktural di tubuh TNI. Model organisasi hierarkis yang lambat dalam pengambilan keputusan perlu digantikan dengan struktur yang lebih adaptif, berbasis tim kecil (*task force*), dan didukung oleh sistem komando digital. Pembentukan unit-unit baru seperti **Cyber Command**, **Rapid Response Task Force**, dan **Information Operations Center** harus diprioritaskan dalam lima tahun mendatang (Lemhannas, 2022).

Selain itu, **pengembangan sumber daya manusia (SDM) digital** menjadi kunci keberhasilan transformasi TNI. Personel TNI perlu dibekali kemampuan *data analytics*, kecerdasan buatan, serta *strategic foresight*. Menurut Raska (2021), militer masa depan akan bergantung pada "*cognitive soldiers*" yang mampu berpikir analitis dan beroperasi dalam lingkungan kompleks berbasis data.

Kurikulum pendidikan militer juga perlu diperbarui agar mencakup **simulasi perang hibrida**, **pelatihan siber**, dan **analisis strategis berbasis data**. Akademi militer dan lembaga pendidikan TNI harus bertransformasi menjadi *learning*

organization yang dinamis, di mana inovasi dan riset teknologi menjadi bagian dari kultur kelembagaan.

4. Integrasi TNI dalam Arsitektur Pertahanan Nasional

a. Pendekatan **Whole-of-Government**

Dalam menghadapi ancaman multidimensi, TNI tidak dapat bekerja secara terisolasi. Diperlukan pendekatan **whole-of-government** yang melibatkan koordinasi lintas kementerian dan lembaga negara. Seperti ditegaskan oleh Nugraha (2023), ketahanan nasional di era perang kontemporer bergantung pada kemampuan pemerintah mengintegrasikan kekuatan militer, diplomasi, ekonomi, dan teknologi secara holistik.

Dalam konteks ini, TNI perlu menjalin kolaborasi strategis dengan **Kemenkominfo** dalam keamanan informasi, **Kemenristek/BRIN** dalam pengembangan teknologi pertahanan, serta **Kemenlu** dalam diplomasi strategis regional. Pendekatan lintas sektor ini memastikan bahwa strategi pertahanan tidak hanya bersifat militeristik, tetapi juga adaptif terhadap perubahan sosial, politik, dan teknologi.

b. Kemandirian Industri Pertahanan

Pembangunan kekuatan TNI juga bergantung pada kemampuan industri pertahanan nasional. UU Nomor 16 Tahun 2012 tentang Industri Pertahanan menegaskan pentingnya kemandirian teknologi melalui pengembangan sistem senjata dalam negeri. Namun, data Kemenhan (2024) menunjukkan bahwa ketergantungan impor masih mencapai lebih dari 50% untuk komponen strategis.

Untuk mengatasi hal ini, diperlukan penguatan kerja sama riset antara TNI, BUMN pertahanan, dan perguruan tinggi. Program *Deftech Innovation Cluster* yang digagas Kemhan dapat menjadi platform kolaboratif dalam mengembangkan sistem drone, sensor, dan AI pertahanan berbasis produksi nasional. Selain meningkatkan

efisiensi, kemandirian industri pertahanan juga memperkuat daya tangkal strategis dan mengurangi kerentanan terhadap embargo luar negeri.

5. Reorientasi Strategi Pertahanan Menuju Kekuatan Adaptif

Perubahan karakter perang menuntut **reorientasi strategi pertahanan nasional** dari pendekatan reaktif menjadi proaktif. Strategi baru harus berfokus pada tiga prinsip utama: **readiness, resilience, dan responsiveness**.

- a. **Readiness** mengacu pada kesiapan operasional TNI dalam menghadapi ancaman multidomain melalui latihan gabungan dan integrasi digital.
- b. **Resilience** menekankan kemampuan pertahanan nasional untuk bertahan dan pulih dari serangan siber atau disinformasi melalui sistem cadangan digital dan komunikasi aman.
- c. **Responsiveness** merujuk pada kecepatan dan ketepatan TNI dalam merespons ancaman melalui *real-time intelligence* dan komando fleksibel.

Selain itu, strategi pertahanan masa depan perlu mengadopsi konsep **deterrence by denial**—yakni mencegah agresi dengan memperkuat kemampuan siber, ruang angkasa, dan informasi. Pendekatan ini lebih sesuai dengan karakter Indonesia yang menganut politik bebas aktif dan strategi pertahanan non-agresif.

6. Sintesis: Arah Transformasi Kekuatan TNI di Era Perang Kontemporer

Berdasarkan analisis di atas, dapat disimpulkan bahwa perang kontemporer telah menggeser paradigma pertahanan nasional dari **hard power** berbasis kekuatan fisik menuju **smart power** berbasis teknologi, informasi, dan adaptivitas. Oleh karena itu, pembangunan kekuatan TNI harus diarahkan pada lima agenda strategis:

- a. **Digitalisasi komando dan kendali (C4ISR)** untuk mendukung operasi lintas domain.

- b. **Pembentukan Cyber Command dan Information Warfare Division** di bawah komando gabungan.
- c. **Modernisasi alutsista berbasis teknologi tinggi**, termasuk integrasi AI dan drone swarm.
- d. **Reformasi pendidikan militer** dengan kurikulum siber, analisis strategis, dan simulasi perang hibrida.
- e. **Sinergi lintas sektor dan industri pertahanan nasional** dalam riset teknologi dan keamanan digital.

Dengan mengadopsi agenda tersebut, TNI akan mampu bertransformasi menjadi kekuatan pertahanan yang **adaptif, responsif, dan kolaboratif** dalam menghadapi ancaman global yang semakin kompleks, tanpa kehilangan karakter dasar sebagai tentara rakyat, tentara pejuang, dan tentara profesional.

Kesimpulan dan Rekomendasi

Kesimpulan

Perang kontemporer telah mengubah secara mendasar cara negara memandang dan mempersiapkan pertahanan nasionalnya. Konflik di abad ke-21 tidak lagi terbatas pada pertempuran fisik, melainkan melibatkan dimensi politik, ekonomi, informasi, dan teknologi yang saling berinteraksi secara simultan. Munculnya perang hibrida, serangan siber, dan perang kognitif menjadikan batas antara masa damai dan perang semakin kabur. Dalam konteks ini, **Tentara Nasional Indonesia (TNI)** dihadapkan pada tuntutan strategis untuk bertransformasi dari kekuatan konvensional menuju **kekuatan multidomain yang adaptif dan berteknologi tinggi**.

Analisis menunjukkan bahwa modernisasi alutsista dan transformasi teknologi menjadi keharusan, namun tidak cukup jika tidak diikuti oleh reformasi doktrin, restrukturisasi organisasi, dan peningkatan kapasitas sumber daya manusia. TNI perlu mengembangkan interoperabilitas antarmatra secara menyeluruh melalui

komando gabungan yang mampu beroperasi dalam ruang darat, laut, udara, siber, dan informasi secara terintegrasi.

Selain itu, perang modern menuntut **pembangunan ekosistem pertahanan digital nasional** yang melibatkan sinergi antara militer, lembaga pemerintah, sektor swasta, dan akademisi. Pendekatan *whole-of-government* menjadi strategi kunci dalam menghadapi ancaman yang multidimensi dan lintas batas. Di sisi lain, kemandirian industri pertahanan nasional menjadi elemen strategis untuk memastikan daya tangkal yang berkelanjutan dan mengurangi ketergantungan eksternal terhadap pasokan senjata dan teknologi.

Pada akhirnya, pembangunan kekuatan TNI harus diarahkan bukan hanya untuk menghadapi ancaman fisik, tetapi juga untuk **menjamin stabilitas informasi, ketahanan siber, dan legitimasi nasional**. Hal ini menegaskan bahwa kekuatan militer di era kontemporer bukan sekadar alat pertahanan, tetapi juga instrumen diplomasi strategis dan stabilitas nasional dalam tatanan global yang semakin kompleks dan tidak menentu.

Rekomendasi

1. Transformasi Doktrin dan Strategi Pertahanan.

Pemerintah dan TNI perlu memperbarui doktrin pertahanan nasional agar mencakup skenario perang hibrida, multidomain, dan perang informasi. Doktrin baru harus menekankan integrasi antara kekuatan konvensional dan non-konvensional berbasis teknologi.

2. Modernisasi Teknologi dan Komando Digital.

Percepatan integrasi sistem komando, kendali, komunikasi, komputer, intelijen, pengawasan, dan pengintaian (*C4ISR*) berbasis kecerdasan buatan perlu menjadi prioritas utama. Hal ini akan memperkuat kemampuan *situational awareness* dan efektivitas operasi militer.

3. **Pembentukan Unit Khusus Siber dan Informasi.**

Diperlukan pembentukan **Cyber Command** dan **Information Warfare Division** yang memiliki mandat ofensif dan defensif dalam menghadapi ancaman siber serta perang kognitif dan disinformasi.

4. **Penguatan SDM Strategis.**

TNI perlu mengembangkan sistem rekrutmen dan pelatihan baru yang berfokus pada keahlian teknologi, *data analytics*, *cyber defense*, dan *strategic foresight*. Kolaborasi dengan universitas dan lembaga riset harus diperluas.

5. **Kemandirian Industri Pertahanan.**

6. Pemerintah harus memperkuat kemitraan antara TNI, BUMN pertahanan, dan sektor swasta nasional untuk mengembangkan teknologi militer dalam negeri, termasuk sistem drone, AI, dan sensor strategis.

7. **Pendekatan Whole-of-Government dan Whole-of-Society.**

Ketahanan nasional di era perang multidomain hanya dapat dicapai melalui koordinasi antara kementerian, lembaga intelijen, industri, dan masyarakat sipil. Kolaborasi lintas sektor akan membangun *national resilience ecosystem* yang tangguh menghadapi ancaman global.

Dengan menerapkan rekomendasi tersebut, **TNI akan mampu bertransformasi menjadi kekuatan pertahanan yang modern, profesional, dan relevan dengan tuntutan geopolitik kontemporer**—sebuah kekuatan yang tidak hanya menjaga kedaulatan, tetapi juga memastikan keberlanjutan dan martabat bangsa di panggung dunia.

Daftar Pustaka

- Alkire, B., Jenkins, S., & Sayler, K. (2020). *Multi-domain operations: Integrating new technologies in defense strategy*. RAND Corporation.
- Arquilla, J., & Ronfeldt, D. (1997). *Networks and netwars: The future of terror, crime, and militancy*. RAND Corporation.

- Badan Siber dan Sandi Negara (BSSN). (2021). *Strategi keamanan siber nasional*. Jakarta: BSSN.
- Bitzinger, R. (2020). *Emerging military technologies and the future of warfare*. International Institute for Strategic Studies.
- Clausewitz, C. von. (1976). *On war* (M. Howard & P. Paret, Eds. & Trans.). Princeton University Press.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage Publications.
- Dibb, P., & Brabin-Smith, R. (2021). *The shape of Australia's defence: Lessons for small and medium powers*. Australian Strategic Policy Institute.
- Farrell, T., & Terriff, T. (2002). *The sources of military change: Culture, politics, technology*. Lynne Rienner Publishers.
- Freedman, L. (2017). *The future of war: A history*. PublicAffairs.
- Galeotti, M. (2022). *The weaponization of everything: The rise of grey-zone conflict*. Yale University Press.
- Gray, C. S. (2010). *Modern strategy* (2nd ed.). Oxford University Press.
- Hoffman, F. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
- Kaldor, M. (2013). *New and old wars: Organized violence in a global era* (3rd ed.). Polity Press.
- Kemhan RI. (2020). *Rencana Strategis Kementerian Pertahanan 2020–2024*. Jakarta: Kementerian Pertahanan Republik Indonesia.
- Krippendorff, K. (2018). *Content analysis: An introduction to its methodology* (4th ed.). Sage Publications.
- Lanoszka, A. (2016). *Russian hybrid warfare and extended deterrence in eastern Europe*. *International Affairs*, 92(1), 175–195.
- Lembaga Ketahanan Nasional (Lemhannas). (2022). *Laporan kajian transformasi pertahanan nasional*. Jakarta: Lemhannas RI.



- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). Sage Publications.
- Nugraha, H. (2023). *Sinergi pertahanan dan keamanan siber dalam kerangka whole-of-government*. *Jurnal Keamanan Nasional*, 8(1), 45–62.
- Nye, J. S. (2019). *Do morals matter? Presidents and foreign policy from FDR to Trump*. Oxford University Press.
- Pusjianstralitbang TNI. (2023). *Kajian strategis transformasi doktrin militer TNI*. Jakarta: Mabes TNI.
- Raska, M. (2021). *Military innovation and adaptation: Technology and doctrine in the Asia-Pacific*. Routledge.
- Ridwan, M. (2022). *Ancaman asimetris dan strategi keamanan nasional Indonesia*. *Jurnal Ilmu Pertahanan*, 9(2), 67–83.
- Singer, P. W. (2010). *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin Press.
- U.S. Army Training and Doctrine Command. (2018). *The U.S. Army in multi-domain operations 2028*. TRADOC Pamphlet 525-3-1.