JURNAL PENDIDIKAN INDONESIA
p-ISSN : 2745-7141 e-ISSN : 2746-1920
Jurnal Pendidikan Indonesia
Vol. 06 No. 11 November 2025

Supremasi Kognitif: Pelajaran dari Kepemimpinan Global untuk Doktrin Pertahanan Siber Indonesia

Mohamad Iswan Nusi, David Mulyadi Cokabo, Tarsisius Susilo, Teguh Heri Susanto, Rudi Firmansyah
Sekolah Staf dan Komando Tentara Nasional Indonesia, Indonesia
Email: iswannusi79@gmail.com, davidcokabo@gmail.com, muchsus70@gmail.com, teguhherisusanto@gmail.com, rufe99@yahoo.co.id

ABSTRAK

Dalam era kompetisi lintas-domain yang semakin kompleks, supremasi kognitif telah menjadi dimensi utama perebutan kekuasaan global. Dominasi tidak lagi ditentukan oleh kekuatan militer semata, tetapi oleh kemampuan negara mengendalikan persepsi, memengaruhi kesadaran publik, dan membentuk realitas sosial melalui teknologi informasi dan algoritma. Penelitian ini bertujuan menganalisis model kepemimpinan strategis Vladimir Putin dan Xi Jinping dalam mengelola ruang kognitif nasional, serta merumuskan implikasinya terhadap pengembangan doktrin pertahanan siber Indonesia. Metode penelitian menggunakan pendekatan kualitatif-analitis dengan teknik studi kepustakaan dan analisis komparatif strategis, berfokus pada integrasi antara teori kekuasaan informasi dan kepemimpinan kognitif. Hasil penelitian menunjukkan bahwa Putin dan Xi berhasil membangun ekosistem kognitif nasional melalui kontrol narasi, penguasaan data, dan orkestrasi teknologi digital untuk memperkuat legitimasi domestik dan menantang hegemonik global. Sebaliknya, Indonesia masih menunjukkan kesenjangan kognitif akibat lemahnya koordinasi kelembagaan, dominasi paradigma teknis, dan ketergantungan terhadap infrastruktur digital asing. Penelitian merekomendasikan pembentukan Doktrin Pertahanan Kognitif Nasional berbasis Pancasila, yang menempatkan kesadaran, kecerdasan strategis, dan integrasi lintas-domain sebagai inti dari kedaulatan siber Indonesia di abad ke-21.

Kata kunci: supremasi kognitif, pertahanan siber aktif, kepemimpinan strategis, perang informasi, kedaulatan kognitif.

Abstract

In the era of increasingly complex cross-domain competition, cognitive supremacy has emerged as the primary dimension of global power rivalry. Dominance is no longer defined merely by military strength but by a state's ability to control perceptions, influence public awareness, and shape social reality through information technology and algorithms. This study aims to analyze the strategic leadership models of Vladimir Putin and Xi Jinping in managing national cognitive space and to formulate their implications for developing Indonesia's active cyber defense doctrine. Using a qualitative-analytical approach with strategic comparative analysis, this research integrates the theories of information power and cognitive leadership. The findings reveal that Putin and Xi have successfully established national cognitive

ecosystems through narrative control, data mastery, and orchestration of digital technologies to strengthen domestic legitimacy and challenge global hegemony. Conversely, Indonesia still experiences a cognitive gap due to institutional fragmentation, overreliance on foreign digital infrastructure, and weak analytical capacity. Therefore, this study recommends developing a ***National Cognitive Defense Doctrine*** *based on Pancasila values, emphasizing strategic awareness, intelligence, and cross-domain integration as the foundation for Indonesia's cognitive sovereignty in the 21st century.*

Keywords: *cognitive supremacy, active cyber defense, strategic leadership, information warfare, cognitive sovereignty.*

LATAR BELAKANG

Dalam era kontemporer yang ditandai oleh kompetisi lintas-domain dan perang informasi yang kian intens, supremasi kognitif (*cognitive supremacy*) telah bergeser menjadi dimensi utama perebutan kekuasaan global antara negara-negara besar seperti Amerika Serikat, Rusia, Tiongkok, dan Israel. Dinamika ini menunjukkan bahwa dominasi tidak lagi semata ditentukan oleh keunggulan militer (*hard powe*r), melainkan oleh kemampuan memengaruhi persepsi, membentuk kesadaran publik, dan mengendalikan arsitektur pengetahuan melalui teknologi informasi dan algoritma pengambilan keputusan (Nye, 2018; Lanoszka, 2020). Kepemimpinan Vladimir Putin dan Xi Jinping menjadi contoh nyata dari penerapan *cognitive leadership* yang mengintegrasikan strategi geopolitik, kontrol narasi, dan manipulasi psikologis dalam setiap pengambilan keputusan strategis (Giles, 2022; Freedman, 2019). Putin, misalnya, memanfaatkan perang kognitif (*cognitive warfare*) untuk membentuk realitas alternatif dalam konflik Ukraina, di mana perang narasi menjadi senjata utama untuk mengonsolidasikan legitimasi domestik sekaligus menantang hegemonik Barat (Ascott, 2020; Horton, 2021; Shuvalova, 2020). Sementara itu, Xi Jinping melalui kebijakan Digital *Silk Road* dan pengembangan *social credit system* berhasil menstrukturkan ulang ruang kognitif warganya melalui integrasi *artificial intelligence dan big data governance* (Creemers, 2017; Triolo & Allison, 2018), menjadikan Tiongkok model negara yang menggabungkan *technological authoritarianism* dengan efisiensi kognitif negara.

Secara normatif, supremasi kognitif semestinya menjadi fondasi konseptual dalam perumusan doktrin pertahanan siber nasional Indonesia. Karena dalam paradigma *cognitive defense*, ancaman tidak hanya dipahami sebagai serangan terhadap infrastruktur digital, tetapi juga terhadap kesadaran dan kemampuan berpikir strategis bangsa (Mankoff, 2021; Tzu, 2010). Oleh karena itu, yang dibutuhkan bukan sekadar *technical superiority*, melainkan *cognitive sovereignty*, yakni kedaulatan berpikir nasional yang menempatkan dimensi moral, ideologis, dan intelektual sebagai bagian dari sistem pertahanan yang terintegrasi. Pancasila sebagai basis nilai harus menjadi kompas epistemik yang menuntun bagaimana teknologi, data, dan informasi digunakan untuk memperkuat ketahanan kognitif bangsa (Darmadi, 2015; Karim, 2018). Di sinilah pentingnya kepemimpinan strategis yang mampu mengombinasikan visi digital, kapasitas analitik, dan integritas nilai. Model kepemimpinan seperti Xi Jinping yang

mengutamakan sinergi antara *national rejuvenation* dan penguasaan data, serta Putin yang mengutamakan kontrol narasi internal, dapat menjadi pembelajaran dalam membangun *cognitive ecosystem* Indonesia yang tahan terhadap penetrasi ideologis eksternal (Giles, 2022; Nye, 2021).

Namun secara empiris, Indonesia masih menghadapi *cognitive gap* yang signifikan antara potensi normatif dan realitas implementasi kebijakan. Pertahanan siber nasional masih lebih bersifat reaktif dan teknis dibandingkan strategis dan konseptual (BSSN, 2023). Fragmentasi kelembagaan, ketergantungan terhadap infrastruktur digital asing, serta rendahnya kapasitas analitik dalam membaca dinamika disinformasi global menunjukkan lemahnya *unity of cognition* antar pemangku kepentingan pertahanan (Haryono, 2022). Di tengah medan perang kognitif yang semakin canggih (di mana a*rtificial intelligence, deepfake propaganda, dan algorithmic manipulation* menjadi senjata utama (Rattray, 2020)) Indonesia berisiko menjadi objek dalam sistem global yang dikendalikan oleh kekuatan besar. Sementara Amerika dan Israel terus memperluas pengaruhnya melalui *cognitive dominance operation*s berbasis *predictive intelligence* (Singer & Brooking, 2018), Tiongkok dan Rusia mengonsolidasikan kekuatan narasi dan kesadaran nasional sebagai bentuk *strategic deterrence*. Kesenjangan ini menegaskan perlunya reposisi doktrin pertahanan siber Indonesia menuju doktrin kognitif yang menekankan kesadaran, kecerdasan strategis, dan integrasi lintas-domain sebagai inti dari keunggulan nasional. Supremasi kognitif, dengan demikian, bukan sekadar target konseptual, melainkan kebutuhan strategis untuk memastikan keberlanjutan kedaulatan Indonesia di tengah arsitektur global yang semakin dikendalikan oleh kekuatan informasi dan kesadaran digital.

Penelitian ini menawarkan pembaruan konseptual dengan memperkenalkan dimensi "kognitif" sebagai inti pertahanan abad ke-21, bukan sekadar perpanjangan dari keamanan siber teknis. Pendekatan ini menempatkan cognitive sovereignty sebagai bentuk kedaulatan baru yang menekankan penguasaan persepsi, kesadaran, dan sistem nilai nasional sebagai elemen utama pertahanan negara. Dengan menganalisis model kepemimpinan strategis Vladimir Putin dan Xi Jinping, penelitian ini membangun model konseptual Doktrin Pertahanan Siber Aktif yang adaptif terhadap konteks Indonesia.

Urgensi penelitian ini terletak pada kebutuhan Indonesia untuk bertransformasi dari paradigma reaktif ke paradigma proaktif dalam menghadapi perang informasi global. Ketika *artificial intelligence*, *deepfake propaganda*, dan *algorithmic manipulation* menjadi senjata utama (Rattray, 2020), ketahanan nasional harus didefinisikan ulang sebagai kemampuan menjaga kesadaran kolektif dan legitimasi politik bangsa. Oleh karena itu, reposisi pertahanan siber menuju pertahanan kognitif menjadi kebutuhan strategis, bukan sekadar agenda kebijakan.

Tujuan penelitian ini adalah merumuskan arah pengembangan Doktrin Pertahanan Siber Aktif Indonesia melalui pembelajaran dari model kepemimpinan strategis global, khususnya Rusia dan Tiongkok. Secara akademis, penelitian ini memperkaya khazanah studi keamanan kontemporer dengan memperluas spektrum analisis dari keamanan teknis ke keamanan kognitif. Secara praktis, hasil penelitian ini diharapkan dapat menjadi referensi bagi Kementerian Pertahanan, TNI, dan BSSN dalam menyusun strategi pertahanan yang berbasis kesadaran dan kecerdasan strategis bangsa.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif strategis dengan paradigma interpretatif-kritis, karena fenomena supremasi kognitif dan perang informasi tidak dapat direduksi hanya pada variabel kuantitatif, melainkan harus dipahami sebagai proses konstruktif yang melibatkan relasi kekuasaan, kepemimpinan, dan persepsi (Creswell, 2018; Denzin & Lincoln, 2017). Pendekatan ini memungkinkan peneliti menafsirkan dinamika *cognitive leadership* Vladimir Putin, Xi Jinping, dan model kepemimpinan Barat dalam konteks perang informasi global, sekaligus menautkannya dengan tantangan struktural dan konseptual yang dihadapi Indonesia dalam membangun doktrin pertahanan siber aktif. Dengan demikian, penelitian ini beroperasi pada dua tataran analisis: (1) level sistem internasional, untuk menelaah pola dan logika supremasi kognitif global, serta (2) level institusional nasional, untuk mengevaluasi kesiapan konseptual dan kelembagaan TNI dalam mengintegrasikan pertahanan informasi ke dalam kerangka doktrin strategis.

Secara metodologis, penelitian ini bersifat deskriptif-analitis dengan desain studi komparatif (*comparative analytical design*), yang membandingkan tiga model kepemimpinan strategis (Putin, Xi, dan Amerika/Barat) berdasarkan kategori analisis, yaitu *epistemic control, decision-making under uncertainty, narrative strategy, dan cognitive infrastructure*. Desain ini kemudian dihubungkan dengan refleksi kritis atas postur pertahanan informasi TNI dan perumusan ulang doktrin pertahanan siber nasional. Data penelitian diperoleh melalui kombinasi studi kepustakaan mendalam (*library research*) terhadap sumber primer dan sekunder, yakni terdiri dari dokumen resmi, pidato kebijakan, laporan strategis pertahanan (DoD, BSSN, Kemhan, RAND, Brookings, CSIS), literatur akademik internasional, serta hasil wawancara mendalam dengan informan kunci di lingkungan TNI, Kemhan, dan BSSN. Teknik penelusuran literatur menggunakan pendekatan critical discourse tracing untuk mengidentifikasi narasi, logika, dan pola argumentasi yang membentuk kebijakan kognitif dan pertahanan informasi di berbagai negara (Fairclough, 2015).

HASIL DAN PEMBAHASAN

Pembahasan terhadap empat rumusan masalah di atas dimaksudkan untuk menelusuri secara sistematis bagaimana dinamika supremasi kognitif dan perang informasi global membentuk arsitektur kepemimpinan, doktrin, serta pertahanan informasi negara-negara besar, dan bagaimana hal tersebut relevan bagi reposisi konseptual pertahanan siber Indonesia. Dalam konteks ini, setiap rumusan masalah tidak berdiri sendiri, melainkan membentuk rantai kausal yang saling berkelindan, yakni dimulai dari perebutan realitas global sebagai ruang perebutan legitimasi, hingga kebutuhan untuk merumuskan ulang doktrin pertahanan nasional yang berorientasi pada kedaulatan kognitif (*cognitive sovereignty*) dan daya tangkal informasi. Dengan demikian, pembahasan diarahkan bukan hanya untuk mendeskripsikan fenomena, melainkan untuk mengkritisi logika kekuasaan yang bekerja di balik konstruksi realitas strategis dan implikasinya bagi *national defense architecture* Indonesia di domain siber.

Pendekatan analisis dalam pembahasan ini bersifat komparatif–kritis, menelaah tiga model kepemimpinan global (Vladimir Putin di Rusia, Xi Jinping di Tiongkok, dan kepemimpinan kolektif Barat (Amerika Serikat dan sekutunya)) dalam mengelola peperangan informasi dan supremasi kognitif. Komparasi ini bukan untuk menilai keunggulan ideologis, melainkan untuk mengidentifikasi pola-pola kepemimpinan strategis dalam pengambilan

keputusan berbasis informasi, manajemen persepsi publik, dan rekayasa kognitif nasional. Melalui kerangka *comparative strategic cognition*, penelitian ini mengurai bagaimana Putin mengoperasionalkan *narrative warfare* sebagai instrumen kontrol domestik dan deterrensi global, Xi Jinping menginstitusionalisasi *data-driven governance* dalam kerangka *otoritarianisme digital*, sementara Amerika dan Israel mengandalkan *technological pluralism dan algorithmic influence* untuk mempertahankan hegemoni informasi. Analisis ini menjadi dasar untuk memahami bagaimana Indonesia perlu mengembangkan kepemimpinan pertahanan yang tidak hanya adaptif terhadap perubahan teknologi, tetapi juga kritis terhadap perang makna yang menyertainya.

Selanjutnya, pembahasan diarahkan pada refleksi mendalam atas postur pertahanan informasi TNI yang saat ini masih berorientasi pada aspek protektif dan reaktif, serta belum sepenuhnya menginternalisasi dimensi kognitif dalam sistem doktrin, organisasi, dan pendidikan pertahanan. Melalui refleksi tersebut, akan dilakukan evaluasi terhadap *unity of cognition*, interoperabilitas sistem informasi, serta kapasitas strategis TNI dalam menghadapi eskalasi perang informasi. Pada tahap akhir, pembahasan berupaya merumuskan arah konseptual doktrin pertahanan siber aktif yang berbasis nilai Pancasila, berorientasi pada sinergi multi-domain, dan mampu membangun daya tangkal strategis melalui penguasaan ruang kognitif. Dengan demikian, pembahasan ini tidak hanya menghasilkan deskripsi analitis, tetapi juga tawaran konseptual untuk membangun arsitektur pertahanan kognitif Indonesia yang berkarakter, berdaulat, dan kompetitif di tengah turbulensi geopolitik informasi global.

Pertempuran untuk memperebutkan realitas di era kepemimpinan global berlangsung, dan sejauh mana dominasi kognitif

Selama hampir dua abad, kerangka Clausewitzian tentang peperangan (yang memandang perang sebagai "kelanjutan politik dengan cara lain") telah mendominasi seluruh lanskap pemikiran strategis dunia. Dalam doktrin klasik tersebut, medan perang diimajinasikan secara fisik: sebagai ruang geospasial yang dapat dipetakan, direbut, dan dikuasai. Clausewitz menempatkan kekerasan bersenjata sebagai instrumen rasional negara untuk memaksakan kehendaknya, dengan medan darat, laut, dan udara sebagai panggung utamanya (Clausewitz, 1832). Namun, memasuki abad ke-21, paradigma ini mengalami disrupsi epistemologis yang mendalam. Munculnya teknologi digital, kecerdasan buatan, dan media jaringan global telah menciptakan domain keempat (dan kini bahkan kelima) dalam peperangan: ruang siber dan ruang kognitif. Dalam konteks ini, teori Clausewitzian perlu direvisi bukan karena usang, melainkan karena ia gagal menjelaskan dinamika perang tanpa kekerasan yang kini memperebutkan kesadaran, bukan teritori. Pertempuran modern tidak lagi berpusat pada kontrol atas ruang fisik, melainkan pada kontrol atas kesadaran sosial, yaitu kemampuan untuk mendefinisikan realitas (*the power to define reality*). Dengan kata lain, **perang kini tidak lagi bersifat geofisik, tetapi geokognitif**, yakni sebuah pertempuran untuk menguasai dimensi persepsi manusia dan menaklukkan kesadaran kolektif masyarakat global.

Transformasi ini membawa implikasi langsung pada konsep kekuasaan. Joseph S. Nye, melalui teori *Information Power*, menegaskan bahwa kekuatan di era digital tidak hanya diukur dari superioritas militer, melainkan dari kapasitas suatu negara untuk memproduksi, memproses, dan mengendalikan arus informasi yang membentuk opini publik serta legitimasi

politik (Nye, 2021). Dalam kerangka ini, informasi bukan lagi variabel pendukung kekuasaan, melainkan inti dari kekuasaan itu sendiri. Negara yang berhasil menguasai arsitektur informasi akan memiliki keunggulan dalam mendefinisikan narasi, membentuk norma, dan memengaruhi preferensi global. Vladimir Putin memahami hal ini secara mendalam. Melalui operasi *information confrontation* dan *reflexive control*, Rusia menargetkan persepsi lawan, bukan hanya sistem senjatanya (Thomas, 2018). *Reflexive control theory* menjelaskan bahwa aktor yang unggul dalam domain kognitif dapat membuat lawan bertindak sesuai kepentingannya sendiri, dengan memanipulasi input persepsi dan data yang diterimanya. Artinya, dominasi strategis bukan diperoleh dari kekuatan koersif, tetapi dari penguasaan terhadap persepsi yang membentuk keputusan musuh. Inilah evolusi logis dari perang Clausewitzian ke **perang persepsi**, di mana kemenangan dicapai bukan melalui penghancuran musuh, tetapi melalui penyesatan pemahamannya.

Sementara itu, Xi Jinping mempraktikkan model yang berbeda namun sama strategis: *cognitive governance*. Xi memandang ruang digital sebagai fondasi legitimasi politik baru, di mana *big data*, *artificial intelligence*, dan sistem *social credit* menjadi alat untuk mengelola kesadaran warganya. Konsep ini memperluas logika Michel Foucault tentang *biopower* menjadi apa yang kini disebut sebagai *infopower*: kekuasaan yang mengatur bukan hanya tubuh dan perilaku, tetapi cara berpikir, menilai, dan mempercayai (Foucault, 1978). Dalam konteks Tiongkok, kekuasaan atas informasi diterjemahkan menjadi mekanisme stabilisasi politik dan konsolidasi ideologis. Xi menjadikan data sebagai infrastruktur kedaulatan nasional, yakni sebuah *data sovereignty regime* yang menempatkan algoritma negara sebagai perpanjangan tangan ideologi Partai Komunis (Creemers, 2017). Dengan demikian, supremasi kognitif di tangan Xi bukanlah hasil dari penetrasi eksternal seperti model Putin, melainkan hasil dari **internalisasi ideologis kolektif** yang dikendalikan secara terpusat. Jika Rusia bertempur dengan *cognitive disruption*, maka Tiongkok bertempur dengan *cognitive order*.

Di sisi lain, Amerika Serikat dan Israel, meskipun memelopori infrastruktur teknologi informasi global, menghadapi dilema yang khas, yaitu **paradoks kebebasan informasi**. Sistem demokrasi liberal yang menjunjung tinggi kebebasan berekspresi justru menjadi celah utama dalam pertahanan kognitifnya. Peter Pomerantsev dalam *This Is Not Propaganda* menjelaskan bahwa *open information systems* dapat berbalik menjadi arena manipulasi jika logika pasar informasi tidak diimbangi oleh etika epistemik (Pomerantsev, 2019). Disinformasi dalam konteks ini bukan sekadar penyebaran berita palsu, tetapi sebuah bentuk *weaponized narrative*, yaitu narasi yang dirancang untuk menciptakan *cognitive overload* dan *emotional dissonance* pada publik sasaran. RAND Corporation memperkuat pandangan ini dengan mengonseptualisasikan *truth decay*, yakni proses sistematis di mana batas antara fakta dan opini menjadi kabur, sehingga kepercayaan publik terhadap institusi runtuh (Helmus, 2018). Ketika informasi menjadi senjata, demokrasi tanpa *cognitive guardrails* justru menjadi korbannya sendiri.

Fenomena disinformasi global inilah yang, menurut François du Cluzel, harus dipahami sebagai bagian integral dari *Cognitive Warfare* yaitu evolusi tertinggi dari *hybrid warfare* yang menargetkan dimensi psikologis dan neurologis manusia (du Cluzel, 2021). Ia mendefinisikan peperangan kognitif sebagai upaya sistematis untuk "menyerang otak" audiens melalui strategi pengaruh, pembingkaian persepsi, dan rekayasa emosional. Berbeda dengan perang siber konvensional yang menyerang sistem teknis, *cognitive warfare* menyerang *decision loop*

manusia, yakni persepsi–analisis–keputusan. Serangan jenis ini, yang dioperasikan melalui media sosial, *deepfake*, dan *bot amplification*, menghasilkan efek destruktif yang lambat namun kumulatif. Ia menggerogoti *centre of gravity* bangsa (legitimasi pemerintah dan kepercayaan sosial) melalui disintegrasi persepsi. Jika senjata nuklir menghancurkan tubuh negara dalam sekejap, maka *cognitive warfare* menghancurkan kesadarannya secara bertahap dan nyaris tanpa disadari.

Sayangnya, hingga kini **postur pertahanan global, termasuk Indonesia, masih cenderung terjebak dalam paradigma defensif yang sempit**. Negara-negara berlomba memperkuat sistem senjata konvensional, sementara "gerbang persepsi" bangsanya dibiarkan terbuka lebar terhadap infiltrasi kognitif. Di Indonesia, alokasi sumber daya pertahanan masih berat pada dimensi kinetik (pada *hard defense instruments)* sementara aspek *soft defense* berupa penguatan literasi digital, kesadaran siber, dan ketahanan kognitif belum menjadi prioritas sistemik (BSSN, 2023). Ketimpangan ini menjadikan bangsa rawan terhadap *asymmetric cognitive penetration*. Alvin dan Heidi Toffler jauh sebelumnya telah memperingatkan bahwa perang di era informasi tidak dimenangkan oleh negara dengan senjata paling kuat, tetapi oleh mereka yang mampu "berpikir lebih cepat daripada lawannya" (Toffler, 1993). Dalam konteks tersebut, Indonesia perlu meninggalkan paradigma reaktif dan beralih pada paradigma *active cognitive defense*, yakni strategi untuk tidak hanya bertahan dari serangan kognitif, tetapi juga membentuk lingkungan persepsi yang menguntungkan bagi kepentingan nasional.

TNI sebagai instrumen pertahanan negara harus menjadi pelopor transformasi ini. Supremasi di medan perang informasi tidak dapat diraih dengan membangun benteng digital yang lebih tinggi, tetapi dengan mengembangkan **arsitektur pertahanan kognitif yang adaptif, ofensif, dan berlandaskan nilai keindonesiaan**. Doktrin Pertahanan Siber Aktif harus didefinisikan bukan sekadar sebagai kebijakan keamanan siber, melainkan sebagai **konsep strategi kebangsaan** yang memadukan *resiliensi Pancasila* dengan kecerdasan buatan, literasi strategis, dan kepemimpinan transformasional. TNI perlu bertransformasi dari *guardian of territory* menjadi *guardian of cognition*, dari penjaga batas fisik menjadi penjaga batas makna. Hanya dengan demikian, Indonesia dapat menavigasi perang makna global dan menegakkan kedaulatan kognitif di tengah pusaran supremasi informasi abad ke-21.

Karakteristik dan perbedaan kepemimpinan strategis Vladimir Putin, Xi Jinping, dan pendekatan kepemimpinan Barat dalam mengelola peperangan informasi

Untuk memahami urgensi perubahan doktrin pertahanan Indonesia, analisis tidak dapat berhenti pada level sistem atau model institusional semata. Yang lebih mendasar adalah bagaimana kepemimpinan strategis di negara-negara adidaya memaknai, mengelola, dan mempersenjatai sumber daya digital serta siber mereka sebagai instrumen kekuasaan nasional. Dalam konteks ini, teori *strategic leadership* sebagaimana dijelaskan oleh Bass (1990) dan Yukl (2013) menegaskan bahwa kepemimpinan bukan sekadar fungsi administratif, melainkan seni mentransformasikan visi menjadi kemampuan adaptif organisasi melalui keberanian mengambil risiko strategis dan membentuk perilaku kolektif. Dalam perang informasi, keputusan, intuisi, serta toleransi risiko dari seorang pemimpin menjadi mekanisme konversi antara potensi teknologi dan daya gempur strategis bangsa. Dengan demikian, memahami

transformasi doktrin pertahanan Indonesia berarti menelusuri logika kepemimpinan yang menafsirkan informasi bukan sebagai alat bantu, tetapi sebagai senjata kebijakan nasional.

a. **Kepemimpinan Vladimir Putin, Memanfaatkan Keterbukaan Demokrasi sebagai Sumber Daya Asimetris**. Kepemimpinan Vladimir Putin menampilkan sintesis unik antara strategi militer klasik Rusia dan inovasi politik kontemporer dalam perang informasi. Melalui prinsip *Reflexive Control Theory*, Putin mempraktikkan kemampuan untuk memengaruhi persepsi lawan agar bertindak sesuai kepentingan Rusia (Thomas, 2018). Ia menyadari bahwa kekuatan konvensional Rusia tidak dapat menandingi Amerika Serikat dan NATO, namun kekuatan asimetris dapat dibangun melalui eksploitasi terhadap *vulnerability of openness* masyarakat demokratis. Putin mengintegrasikan badan-badan intelijen seperti FSB dan GRU dalam sebuah arsitektur informasi negara yang non-linear. Lahirnya entitas seperti *Internet Research Agency* (IRA) menjadi wujud konkret dari kepemimpinan yang mentransformasi sumber daya manusia non-tradisional (troll, peretas, dan propagandis) menjadi bagian dari mesin negara. Pendekatan ini menunjukkan pola kepemimpinan yang adaptif terhadap kompleksitas, sebagaimana dijelaskan oleh teori adaptive leadership Heifetz (1994), yakni pemimpin efektif bukan yang menolak disrupsi, tetapi yang memanfaatkannya sebagai peluang strategis. Keputusan Putin untuk melakukan intervensi masif terhadap Pemilu AS 2016 menandai tingkat toleransi risiko yang tinggi. Ia menyadari bahwa dalam domain digital, atribusi serangan bersifat ambigu dan plausible deniability menjadi perisai politik yang efektif. Putin melihat media sosial bukan sebagai ancaman, melainkan sumber daya publik Barat yang dapat dikonversi menjadi infrastruktur pengaruh Rusia. Pelajaran bagi Indonesia jelas: dalam perang informasi, superioritas teknologi bukanlah determinan utama. Kemenangan ditentukan oleh kapasitas kognitif kepemimpinan untuk memahami psikologi sosial, kultur politik, dan perilaku informasi masyarakat lawan. Tanpa doktrin kognitif yang kuat, kebebasan dan keterbukaan bangsa dapat menjadi "senjata makan tuan" yang dieksploitasi oleh kekuatan eksternal.
b. **Kepemimpinan Xi Jinping, Kontrol Epistemik sebagai Basis Kedaulatan Digital**. Berbeda dengan pendekatan Putin yang bersifat disrupsi, Xi Jinping menampilkan paradigma kepemimpinan yang berlandaskan pada *total information control*, yaitu sebuah bentuk kekuasaan yang menggabungkan ideologi, teknologi, dan otoritas hukum dalam satu ekosistem. Visi besar Xi tentang *The Great Rejuvenation of the Chinese Nation* bergantung pada apa yang disebut Foucault (1978) sebagai *knowledge-power nexus*, yaitu kekuasaan sejati bersumber dari kemampuan mengendalikan pengetahuan dan arus informasi. Melalui kebijakan *Civil-Military Fusion*, Xi mengintegrasikan industri sipil dan militer menjadi satu sistem keamanan nasional berbasis data. Raksasa teknologi seperti Huawei, Alibaba, dan Tencent diwajibkan secara hukum untuk mendukung operasi intelijen negara. Data pengguna WeChat atau TikTok bukan sekadar catatan privat, tetapi dikonseptualisasikan sebagai aset strategis negara. Ini merefleksikan apa yang disebut Morozov (2019) sebagai digital statism, yakni negara yang memonopoli data sebagai instrumen kedaulatan. Lebih jauh, Xi secara pribadi memimpin *Central Cyberspace Affairs Commission*, menandakan bahwa pengelolaan siber bukan domain teknokrat semata, tetapi instrumen kekuasaan politik tertinggi. Ia melahirkan legislasi seperti *Cybersecurity Law* (2017) dan *Data Security Law* (2021) yang meneguhkan kedaulatan data nasional. Model ini memperlihatkan kepemimpinan yang memadukan *technocratic authoritarianism* (Creemers, 2017) dengan

efisiensi strategis. Pelajaran bagi Indonesia adalah perlunya kepemimpinan nasional yang memiliki kesadaran epistemik, yakni memahami bahwa data warga negara adalah infrastruktur kedaulatan yang sama pentingnya dengan wilayah fisik. Tanpa arah strategis dan visi politik yang kuat, kedaulatan digital Indonesia akan terus bergantung pada arsitektur asing yang tidak berpihak pada kepentingan nasional.

c. **Kepemimpinan Amerika Serikat dan Israel, Inovasi Strategis dan Agresivitas Terukur**. Sementara Rusia dan Tiongkok menonjolkan kontrol dan disrupsi, negara-negara demokratis seperti Amerika Serikat dan Israel menunjukkan model kepemimpinan yang menyeimbangkan antara inovasi strategis dan agresivitas terukur. Di AS, evolusi menuju doktrin *Defend Forward* tidak lahir secara spontan, tetapi melalui kontinuitas kepemimpinan di Pentagon dan Gedung Putih yang berani mengoreksi kegagalan paradigma pertahanan pasif. Pembentukan U.S. *Cyber Command* sebagai *unified combatant command* pada 2018 mencerminkan penerapan teori *transformational leadership* Bass (1990), yaitu pemimpin yang memotivasi perubahan budaya organisasi dari reaktif menuju ofensif, dengan memberikan otonomi taktis kepada operator siber untuk melakukan operasi pre-emptive. Israel, dengan konteks ancaman eksistensial yang konstan, menampilkan model kepemimpinan yang berbasis *innovation-centric defense*. Unit elit 8200 menjadi simbol *strategic incubation system* di mana talenta militer muda dikembangkan menjadi aktor inovatif yang kemudian mendirikan perusahaan-perusahaan keamanan siber kelas dunia. Ini adalah bentuk kepemimpinan yang memadukan militerisme dan kewirausahaan, yaitu sebuah ekosistem national *innovation defense* (Even & Shany, 2020). Model ini memperlihatkan bahwa pertahanan siber di negara demokratis tidak harus diartikulasikan sebagai *state monopoly of force*, melainkan sebagai whole-of-nation effort yang melibatkan pemerintah, industri, dan akademia. Pelajarannya bagi Indonesia: kepemimpinan pertahanan harus berfungsi sebagai *network orchestrator*, bukan sekadar pengendali birokratis, yakni membangun ekosistem inovasi nasional yang memadukan kreativitas sipil dan disiplin militer.

d. **Sintesis dan Urgensi bagi Indonesia, Menuju Doktrin Pertahanan Siber Aktif Berbasis Nilai**. Analisis di atas menegaskan bahwa pengelolaan sumber daya digital dan siber tidak pernah bersifat teknis semata; ia adalah keputusan politik tertinggi yang mencerminkan filosofi kekuasaan dan visi kebangsaan. Putin mempersenjatai keterbukaan, Xi mempersenjatai kontrol, sementara Amerika Serikat dan Israel mempersenjatai inovasi serta ketangkasan adaptif. Bagi Indonesia, sintesis dari ketiganya harus diartikulasikan dalam bentuk Doktrin Pertahanan Siber Aktif yang berkarakter Indonesiawi, yakni berakar pada Pancasila, berpijak pada kedaulatan digital, dan berorientasi pada daya tangkal kognitif. Doktrin ini harus menempatkan data sebagai sumber daya nasional, talenta digital sebagai *strategic human capital*, dan ruang informasi sebagai domain kedaulatan baru yang tak kalah penting dari darat, laut, udara, dan ruang angkasa. Sebagaimana ditegaskan oleh Huntington (1957), esensi kepemimpinan militer bukan sekadar kemampuan bertempur, tetapi kemampuan untuk menerjemahkan nilai politik negara ke dalam strategi pertahanan yang efektif. Dengan demikian, kepemimpinan nasional Indonesia harus memimpin transformasi ini melalui keberanian politik, visi epistemik, dan kemampuan integratif lintas-sektor. Tanpa keberanian untuk melangkah ke arah tersebut, maka seluruh upaya reformasi doktrin hanya

akan menjadi *strategic rhetoric*, yaitu menghasilkan kebijakan yang tampak kuat di atas kertas, namun lemah dalam implementasi.

Postur pertahanan informasi TNI saat ini jika dihadapkan dengan eskalasi perang kognitif global

Dengan latar belakang peta jalan peperangan global yang semakin bergeser dari ranah fisik menuju ranah kognitif, Indonesia dihadapkan pada keharusan untuk melakukan refleksi strategis dan epistemologis terhadap struktur, doktrin, serta kultur pertahanan informasi yang dimiliki TNI saat ini. Fenomena perang informasi global bukan lagi isu pinggiran dalam studi keamanan, melainkan inti dari arsitektur kekuasaan modern yang menentukan daya tangkal sebuah negara. Dalam paradigma *cognitive warfare*, sebagaimana dijelaskan oleh du Cluzel (2021), serangan terhadap kesadaran kolektif, persepsi publik, dan legitimasi institusional kini menjadi bentuk baru dari agresi lintas-domain. Dalam konteks ini, TNI sebagai tulang punggung sistem pertahanan negara harus menggeser orientasi konseptualnya, yaitu dari paradigma "pengamanan jaringan" menuju paradigma "penguasaan makna". Namun untuk sampai ke sana, diperlukan keberanian intelektual untuk mengakui bahwa terdapat tiga diskoneksi strategis fundamental dalam postur pertahanan informasi saat ini, yang bukan semata-mata masalah operasional, tetapi menyangkut struktur berpikir, mandat hukum, dan desain kelembagaan. Ketiga diskoneksi itu adalah diskoneksi tempo, mandat, dan sinergi, yakni tiga poros yang menentukan sejauh mana TNI mampu memimpin perang kognitif, bukan sekadar meresponsnya.

a. **Diskoneksi Tempo, Paradigma Reaktif dalam Ekosistem Perang Instan**. Diskoneksi pertama dan paling mendasar terletak pada ketertinggalan tempo strategis. Dalam konteks perang informasi, waktu bukan sekadar dimensi teknis, tetapi variabel strategis yang menentukan siapa yang mengendalikan realitas. Menurut Alvin dan Heidi Toffler (1993), kecepatan berpikir dan kecepatan bereaksi adalah faktor pembeda antara pemenang dan pecundang dalam era "*third wave warfare*." Namun hingga kini, pola operasi informasi TNI masih beroperasi dalam kerangka reaktif dan linier, yaitu respon yang terjadi setelah ancaman teridentifikasi, bukan sebelum muncul. Struktur birokrasi komando yang hierarkis menyebabkan keterlambatan dalam deteksi dan respons. Ketika narasi disinformasi viral di media sosial, rantai koordinasi antarfungsi (Siber, Bais, Puspen) baru bergerak setelah kerusakan persepsi publik sudah meluas. Pola seperti ini menjadikan TNI terjebak dalam perang narasi yang selalu defensif, yakni menanggapi, bukan mendefinisikan. Dalam istilah Clausewitz modern, TNI kehilangan "*centre of gravity*" bukan karena lemahnya daya tempur, tetapi karena kehilangan kemampuan untuk mengatur tempo dan menentukan konteks makna. Lebih parah lagi, sistem monitoring informasi yang ada masih didominasi oleh pattern recognition berbasis kuantitas (menghitung intensitas tagar atau *trending topic*) tanpa mekanisme *cognitive anticipation* untuk memprediksi arah pergeseran narasi. Padahal, menurut Gray (2010), kemenangan strategis dalam domain informasi ditentukan oleh kemampuan membangun keunggulan temporal, yaitu memukul lebih cepat, menafsir lebih dini, dan mengarahkan persepsi sebelum lawan menstrukturkan makna. Dengan kata lain, TNI saat ini masih berperang dengan "jam mekanis", sementara lawan menggunakan "jam algoritmik." Ketimpangan tempo inilah yang membuat setiap respon resmi, betapapun faktual, selalu kalah resonansi dibanding kebohongan yang lebih dulu menyebar. Karena itu,

transformasi doktrin harus menempatkan *tempo supremacy* sebagai elemen inti, yakni kemampuan melakukan deteksi dini narasi, intervensi cepat terhadap ruang publik digital, dan orkestrasi kontra-narasi secara simultan lintas-domain sebelum momentum strategis berpindah ke pihak lawan.

b. **Diskoneksi Mandat, Ambiguitas Doktrinal di Tengah Perang Tanpa Batas**. Diskoneksi kedua bersifat normatif dan konseptual: yakni ketidakjelasan mandat doktrinal TNI dalam domain siber dan informasi. Secara kelembagaan, fungsi TNI dalam menghadapi ancaman informasi masih ditafsir secara konservatif, terbatas pada perlindungan jaringan internal dan diseminasi kegiatan positif. Tafsir ini berakar pada paradigma lama pertahanan, yakni bahwa ancaman harus bersifat fisik, terukur, dan datang dari luar batas negara. Padahal, dalam perang kognitif, ancaman terbesar justru bersifat internal, psikologis, dan tanpa bentuk. Konsep *borderless warfare* sebagaimana dikemukakan oleh Qiao Liang dan Wang Xiangsui (1999) menunjukkan bahwa batas antara perang dan damai telah runtuh; aktor non-negara kini dapat melancarkan agresi strategis tanpa menembakkan peluru. Dalam konteks ini, mandat TNI yang masih dibatasi oleh interpretasi "pertahanan terhadap serangan fisik" menjadi *anachronistic,* yakni tidak mampu menjawab logika ancaman yang bersifat "*non-kinetic but decisive*."Tanpa keberanian untuk memperluas mandat, TNI akan terus berperang dalam kerangka legal yang terbelakang dari dinamika ancaman. Musuh tidak lagi menyerang pangkalan militer, tetapi menyerang kesadaran nasional: memecah kepercayaan publik, membentuk polarisasi sosial, dan melemahkan integrasi ideologis bangsa melalui arsitektur media digital. Disinformasi bukan hanya instrumen propaganda, tetapi senjata psikologis untuk menghancurkan moral cohesion bangsa dari dalam. Karenanya, mandat baru pertahanan informasi harus mencakup operasi kontra-informasi proaktif (*offensive information operation*), yaitu kemampuan untuk melacak, mengintervensi, dan melumpuhkan jaringan penyebar disinformasi baik di dalam maupun luar negeri. Dalam perspektif Huntington (1957), militer yang profesional tidak diukur dari seberapa sempit ia menaati batas hukum, tetapi dari seberapa dalam ia memahami *raison d'être* keberadaannya, adalah menjaga eksistensi negara dari segala bentuk ancaman, termasuk yang tak kasat mata. TNI perlu memimpin redefinisi tersebut dengan keberanian intelektual dan landasan moral yang kuat, yakni agar pertahanan informasi menjadi bukan sekadar fungsi teknis, tetapi alat eksistensial kedaulatan bangsa.

c. **Diskoneksi Sinergi, Silo Struktural di Era Peperangan Terintegrasi.** Diskoneksi ketiga bersifat struktural dan kultural, yakni lemahnya sinergi lintas-domain di antara unit-unit pertahanan informasi. Dalam paradigma perang modern, sebagaimana dijelaskan dalam *Joint Operations Doctrine* (JP 3-0), kemenangan hanya dapat dicapai melalui integrasi antardomain (darat, laut, udara, siber, dan kognitif) dalam satu *unity of effort*. Namun, postur TNI saat ini masih merefleksikan logika organisasi industrial abad ke-20, yakni fungsi-fungsi berjalan dalam silo, bukan dalam ekosistem integratif. Bais berfokus pada deteksi dan analisis ancaman strategis; Siber TNI beroperasi dalam domain teknis; sementara Puspen dan unit penerangan angkatan berperan dalam komunikasi publik. Sayangnya, tidak ada mekanisme yang bersifat institutionalized untuk memastikan hasil intelijen langsung dioperasionalkan menjadi langkah kontra-informasi atau strategi naratif terpadu. Akibatnya, informasi strategis kerap berhenti di meja analisis tanpa diubah menjadi tindakan. Lebih

jauh, ketiadaan joint cognitive operations center menjadikan setiap fungsi berjalan dengan orientasi sektoral, bukan sistemik. Padahal, seperti ditekankan oleh Builder (1989), efektivitas organisasi militer modern terletak pada kemampuannya membangun information *fusion architecture*, yakni sistem yang mampu mengintegrasikan data, narasi, dan psikologi publik dalam satu jaringan keputusan yang cepat. Kebijakan luar negeri Indonesia yang menganut prinsip "bebas aktif" memperkuat kecenderungan berhati-hati dalam domain informasi. Namun dalam konteks perang kognitif global, sikap "hati-hati" sering diterjemahkan oleh lawan sebagai *vacuum of deterrence*, yakni ruang kosong yang dapat dimasuki oleh narasi asing. Laksmana (2020) menyebut hal ini sebagai "ambiguitas strategis Indonesia": posisi yang tampak netral, namun dalam praktiknya rentan terhadap penetrasi informasi lintas-negara. Maka, tantangan utama bukan sekadar membentuk lembaga baru, tetapi membangun budaya sinergi doktrinal, yakni di mana setiap fungsi, dari analisis hingga komunikasi publik, beroperasi dalam logika yang sama: memenangkan persepsi. Dalam konteks perang informasi, tidak ada garis depan tunggal; seluruh masyarakat adalah front, dan seluruh ruang digital adalah medan tempur.

d. **Reformulasi Arah Doktrin, Menuju Pertahanan Informasi Proaktif dan Terintegrasi**. Ketiga diskoneksi strategis tersebut mencerminkan satu problem epistemik besar, yakni TNI belum memandang informasi sebagai domain perang yang otonom dan menentukan. Paradigma yang masih menempatkan informasi sebagai pelengkap operasi fisik menghambat transformasi menuju information-*dominant defense*. Padahal, dalam realitas strategis saat ini, informasi adalah senjata, persepsi adalah wilayah, dan kesadaran publik adalah medan pertempuran. Untuk menutup ketiga diskoneksi tersebut, diperlukan reformulasi doktrin pertahanan informasi dan siber aktif yang menempatkan tiga poros utama sebagai pilar:
   1) Supremasi Tempo (*Tempo Supremacy*), yaitu membangun kemampuan deteksi dini narasi, intervensi cepat, dan manuver naratif berbasis intelijen prediktif.
   2) Kejelasan Mandat (*Mandate Clarity*), yaitu memastikan payung hukum, politik, dan etika yang memungkinkan TNI beroperasi ofensif dalam domain kognitif dengan legitimasi penuh.
   3) Integrasi Sistemik (*Systemic Integration*), yaitu menciptakan struktur komando lintas-fungsi yang memadukan intelijen, operasi siber, komunikasi strategis, dan riset sosial dalam satu sistem pengambilan keputusan.

Seperti dikemukakan Gray (2010), kemenangan strategis dalam abad informasi bukan ditentukan oleh siapa yang memiliki senjata lebih canggih, tetapi siapa yang lebih cepat berpikir secara sistemik dan bertindak secara terpadu. TNI, dengan tradisi intelektual dan disiplin organisasionalnya, memiliki fondasi untuk menjadi pelopor pertahanan informasi nasional, yakni asal berani meninggalkan paradigma reaktif dan mengadopsi doktrin kognitif yang berpijak pada realitas perang modern. Dengan demikian, revolusi pertahanan informasi TNI tidak hanya akan memperkuat ketahanan nasional, tetapi juga membentuk kesadaran baru bahwa kedaulatan di abad ke-21 bukan lagi tentang batas teritorial, melainkan tentang kemampuan sebuah bangsa untuk menentukan, memaknai, dan mempertahankan realitasnya sendiri.

Merumuskan Ulang Doktrin sebagai Arsitektur Pertahanan Siber Aktif untuk TNI

Untuk menjembatani ketiga diskoneksi strategis yang telah diuraikan sebelumnya (yakni tempo, mandat, dan sinergi) dibutuhkan lebih dari sekadar penyesuaian inkremental. Yang dibutuhkan adalah lompatan konseptual dan paradigmatik yang bersifat transformatif, bukan kosmetik. TNI tidak hanya harus menyesuaikan prosedur dan sistemnya, tetapi juga mengubah cara berpikir tentang perang itu sendiri. Dalam kerangka teori *anticipatory governance* (Beck, 2009), institusi yang ingin bertahan di lingkungan strategis berisiko tinggi harus mampu bergerak dari reaksi ke antisipasi, dari proteksi ke pre-emption, dan dari pertahanan pasif menuju pertahanan aktif. Dengan demikian, arah baru yang diperlukan adalah perumusan Doktrin Pertahanan Siber Aktif (*Active Cyber Defense Doctrine*), yakni sebuah konsep operasional dan normatif yang menggabungkan logika strategis, etika hukum internasional, dan kemampuan teknologi nasional ke dalam satu arsitektur pertahanan yang proaktif, fleksibel, dan berdaya tangkal tinggi.

Penting untuk digarisbawahi secara tegas bahwa Pertahanan Aktif bukanlah lisensi untuk agresi tanpa batas. Paradigma ini tidak melegitimasi serangan pre-emptif atau tindakan ofansif yang melanggar hukum perang internasional. Sebaliknya, ia merupakan kerangka kerja strategis yang disiplin, terukur, dan akuntabel, yaitu sebuah *rules-based proactive defense architecture* yang memungkinkan TNI untuk mengidentifikasi, melacak, mengganggu, dan menetralisir ancaman di luar perimeter jaringan nasional sebelum ancaman tersebut menembus sistem vital pertahanan negara. Dalam istilah *strategic studies*, ini adalah transisi dari fortress mentality menuju *mobile cognitive defense*, di mana TNI tidak lagi sekadar menjaga tembok digital, tetapi melakukan patroli tempur kognitif untuk mengamankan ruang informasi dan persepsi nasional. Filosofi dasarnya bergeser dari "bertahan di benteng" menjadi "mengendalikan wilayah kesadaran" di luar batas fisik, menempatkan TNI sebagai aktor dominan dalam siklus persepsi global.

Untuk menopang arsitektur konseptual tersebut, doktrin baru ini harus dibangun di atas tiga pilar fundamental yang saling berkelindan dan saling memperkuat, sebagaimana struktur doktrin perang modern, yaitu intelijen prediktif berbasis fusi, operasi kontra-narasi yang dinamis, dan aplikasi efek siber yang presisi. Ketiga pilar ini bukan entitas terpisah, melainkan sistem ekologi strategis, yakni di mana output dari satu pilar menjadi input bagi pilar lain, menghasilkan siklus adaptif yang terus memperbarui keunggulan kognitif Indonesia di tengah konstelasi perang informasi global.

a. **Pilar Pertama. Intelijen Prediktif Berbasis Fusi (*Fusion-Based Predictive Intelligence*).** Pilar pertama adalah jantung doktrin, yakni intelijen prediktif yang terintegrasi lintas-domain. Dalam era di mana data menjadi amunisi baru, kemampuan untuk memprediksi niat jauh lebih penting daripada sekadar mendeteksi peristiwa. Teori *cognitive dominance* menegaskan bahwa keunggulan strategis diperoleh bukan melalui superioritas senjata, tetapi melalui kecepatan dalam memahami dan memproyeksikan pola tindakan lawan (Rattray, 2020). Oleh karena itu, sistem intelijen TNI harus berevolusi dari model deskriptif-reaktif menuju model prediktif-preskriptif, yang tidak hanya menjawab "apa yang terjadi", tetapi juga "apa yang akan terjadi dan bagaimana kita harus meresponsnya."Pendekatan *Fusion Intelligence* menuntut penyatuan data dari seluruh disiplin, yaitu SIGINT (intelijen sinyal), OSINT (sumber terbuka), HUMINT (manusia), dan CYBINT (siber), yang diolah secara real-time oleh algoritma kecerdasan buatan. *Teknologi*

machine learning dan natural *language processing* dapat digunakan untuk mendeteksi pola penyebaran disinformasi, mengidentifikasi akun bot, menilai intensitas emosi dalam percakapan daring, dan bahkan memperkirakan *psychological vulnerability* dari populasi target. Hasilnya bukan sekadar laporan analitik, melainkan peta kognitif dinamis, yaitu sebuah situational *awareness matrix* yang menggambarkan hubungan antaraktor, jaringan distribusi narasi, dan spektrum motif yang melatarbelakangi operasi informasi musuh. Dalam konteks TNI, peta kognitif ini menjadi instrumen komando strategis yang memungkinkan para pemimpin untuk mengambil keputusan berdasarkan prediksi, bukan asumsi. Dengan memadukan analisis kuantitatif dan kualitatif, pilar ini memungkinkan TNI mengadopsi pola pikir OODA loop (*Observe–Orient–Decide–Act*) yang lebih cepat daripada lawan (Boyd, 1987), yakni memampukan TNI mengamati tren informasi, menyesuaikan orientasi strategis, memutuskan tindakan naratif, dan melaksanakannya sebelum lawan menyadari adanya perubahan.

b. **Pilar Kedua. Operasi Kontra-Narasi Dinamis dan Multi-Lapis (*Dynamic, Multi-Layered Counter-Narrative Operations*).** Intelijen prediktif hanya akan memiliki nilai strategis jika diterjemahkan menjadi tindakan naratif yang presisi. Pilar kedua menegaskan pentingnya kemampuan TNI untuk mengendalikan lanskap makna melalui operasi kontra-narasi yang simultan, adaptif, dan berlapis. Dalam teori narrative warfare (Pomerantsev, 2019), kekuasaan di era digital bergantung pada siapa yang mampu mendefinisikan realitas sosial terlebih dahulu. Dengan demikian, pertahanan informasi tidak lagi cukup dengan klarifikasi birokratis; ia membutuhkan seni manuver persepsi. Operasi kontra-narasi yang dinamis mencakup empat spektrum aksi:
   1) *Pre-bunking* (inokulasi naratif). TNI menanamkan kekebalan kognitif di masyarakat melalui edukasi publik, kampanye kesadaran digital, dan penyebaran konteks faktual sebelum narasi musuh muncul. Ini sejalan dengan konsep *psychological inoculation theory* (McGuire, 1964) yang menegaskan bahwa audiens yang telah "divaksinasi" terhadap manipulasi lebih resisten terhadap propaganda.
   2) *Counter-messaging*. Ketika narasi musuh telah menyebar, tanggapannya bukan sekadar bantahan rasional, melainkan peluncuran narasi tandingan yang emosional, empatik, dan resonan dengan nilai kebangsaan. Disinilah *strategic communication* bertemu dengan behavioral insight, yakni narasi tandingan harus lebih menggugah daripada sekadar benar.
   3) Amplifikasi strategis. Melibatkan masyarakat sipil, akademisi, dan tokoh keagamaan sebagai force multiplier dalam membangun daya tangkal naratif bangsa. Hal ini mencerminkan pendekatan *whole-of-nation* yang diadopsi banyak negara dalam domain kognitif (NATO, 2020).
   4) Dekomposisi narasi musuh. Analisis terbuka terhadap logika disinformasi, pembongkaran motif, serta eksposisi sistematis atas manipulasi yang dilakukan lawan, yakni mendorong publik bukan hanya menolak narasi palsu, tetapi memahami mekanisme di baliknya. Melalui mekanisme multi-lapis ini, TNI berperan bukan hanya sebagai pelindung informasi, tetapi sebagai arsitek kesadaran nasional, memastikan narasi yang membentuk opini publik tetap selaras dengan nilai-nilai Pancasila, kepentingan strategis negara, dan keamanan kognitif bangsa.

c. **Pilar Ketiga. Aplikasi Efek Siber Presisi dan Terukur (*Precise and Scalable Cyber Effects Application*).** Pilar ketiga merupakan dimensi instrumental dan teknologis dari

doktrin ini: kemampuan untuk menerapkan efek siber yang presisi, terkendali, dan dapat disangkal (*plausible*) guna mendukung operasi intelijen dan kontra-narasi. Dalam paradigma *active cyber defense* (Lin, 2016), pertahanan yang efektif menuntut kombinasi antara deteksi dini, respons aktif, dan kemampuan ofensif terbatas yang berorientasi defensif. Artinya, TNI harus memiliki kemampuan untuk mengganggu, menurunkan efektivitas, dan menonaktifkan infrastruktur musuh yang digunakan untuk menyerang kesadaran publik Indonesia, tanpa melanggar norma hukum internasional. Spektrum efek siber ini bersifat eskalatif dan terukur:

1) Tingkat Rendah (Disrupsi). Penghentian sementara operasi botnet, spam farm, atau *fake-account cluster* yang menjadi mesin penyebar disinformasi.
2) Tingkat Menengah (Degradasi). Penurunan performa server penyebar propaganda melalui serangan siber legal dan *traffic flooding* terkontrol.
3) Tingkat Tinggi (Netralisasi). Penonaktifan pusat komando dan kontrol (C2) musuh dalam keadaan darurat strategis, seperti kampanye yang berpotensi memicu kerusuhan sosial atau konflik horizontal.

Setiap tindakan di bawah pilar ini harus tunduk pada rules of engagement yang ketat, berada dalam kendali gabungan sipil-militer, dan dapat diaudit secara hukum serta etika strategis. Prinsip dasarnya adalah "proaktif tanpa provokasi", yakni mempertahankan stabilitas dengan melakukan intervensi cerdas dan terukur sebelum eskalasi terjadi.

d. **Implementasi Doktrin. Revolusi Kognitif dan Reformasi Organisasi.** Penerapan ketiga pilar tersebut menuntut revolusi kelembagaan dan budaya militer. Doktrin baru ini tidak akan efektif tanpa perubahan struktural menuju pembentukan Gugus Tugas Operasi Informasi Terpadu (*Integrated Information Operations Task Force*), yakni unit permanen yang mengonsolidasikan analis intelijen, operator siber, psikolog militer, dan pakar komunikasi strategis dalam satu fusion command structure. Ini mencerminkan model *Cyber Mission Force AS atau Information Warfare Division* Australia, yang mengintegrasikan fungsi kognitif, teknologis, dan psikologis ke dalam satu kerangka komando. Lebih jauh lagi, sistem pendidikan militer Indonesia harus turut berevolusi. Akademi Militer, Sesko Angkatan, Sesko TNI, dan Lemhannas perlu membentuk jalur pembelajaran baru untuk mencetak "Perwira Kognitif" (*Cognitive Officers*), yakni perwira yang tidak hanya memahami strategi perang konvensional, tetapi juga mahir dalam membaca pola naratif, analitik data, psikologi massa, dan komunikasi strategis. Sebagaimana dikatakan Senge (1990), organisasi unggul adalah organisasi yang belajar lebih cepat dari lingkungannya; maka TNI harus menjadi *learning defense organization* yang mampu menyesuaikan diri terhadap disrupsi informasi secara berkelanjutan. Dengan menerapkan Doktrin Pertahanan Siber Aktif berbasis tiga pilar tersebut, TNI tidak hanya memperkuat postur pertahanannya, tetapi juga menegakkan kedaulatan kognitif bangsa, yakni sebuah bentuk baru dari national power yang tak kalah strategis dari kekuatan militer konvensional. Dalam dunia di mana peperangan ditentukan bukan oleh siapa yang menembak lebih dulu, tetapi oleh siapa yang mendefinisikan kebenaran lebih dulu, kemampuan untuk berpikir lebih cepat, bertindak lebih presisi, dan berkoordinasi lintas-domain menjadi bentuk tertinggi dari pertahanan nasional.

KESIMPULAN

Indonesia tengah menghadapi titik balik sejarah pertahanan nasional, di mana kedaulatan tidak lagi diukur dari kekuatan militer semata, tetapi juga dari kemampuan bangsa mempertahankan kemandirian kognitif dan integritas informasional. Dalam era peperangan informasi yang berlangsung di ruang digital dan kognitif, ancaman terhadap kesadaran kolektif dan legitimasi politik menjadi sama berbahayanya dengan serangan bersenjata. Karena itu, reorientasi menuju Doktrin Pertahanan Siber Aktif menjadi keniscayaan strategis. Pada tingkat strategis, diperlukan penyusunan *Buku Putih Doktrin Peperangan Informasi Nasional* sebagai panduan utama bagi pengembangan kebijakan, kapabilitas, dan pendidikan militer agar Indonesia bersikap proaktif dalam menghadapi konflik informasi global. Pada tingkat operasional, TNI harus mengintegrasikan skenario perang informasi multidomain dalam latihan militer guna meningkatkan interoperabilitas sistem siber dan kemampuan kontra-narasi strategis. Pada tingkat kelembagaan, pemerintah dan DPR perlu membentuk Koalisi Keamanan Nasional untuk Reformasi Hukum Siber dan Informasi guna memperbarui regulasi seperti UU ITE, UU Pertahanan Negara, dan UU Intelijen agar sesuai dengan kebutuhan peperangan informasi modern, disertai pembentukan Gugus Tugas Operasi Informasi Terpadu yang melibatkan TNI, BSSN, BIN, dan Kemenkomdigi. Masa depan pertahanan Indonesia tidak ditentukan oleh jumlah alutsista, melainkan oleh kemampuan menguasai medan perang atas makna, persepsi, dan kebenaran. Dengan bertransformasi melalui Doktrin Pertahanan Siber Aktif, TNI bukan hanya pelindung teritori, tetapi juga penjaga kesadaran nasional—menjadi pedang yang cerdas, presisi, dan berakar pada Pancasila untuk memastikan Indonesia tetap berdaulat, berpikir, dan memimpin di tengah gempuran informasi global.

DAFTAR PUSTAKA

Ascott, T. (2020). This is not propaganda: Adventures in the war against reality. *The RUSI Journal, 165*(1). https://doi.org/10.1080/03071847.2020.1731155

Badan Siber dan Sandi Negara (BSSN). (2023). *Laporan tahunan keamanan siber nasional 2023*. Jakarta: BSSN.

Clausewitz, C. von. (1832). *On war*. Berlin: Dümmlers Verlag.

Creemers, R. (2017). Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China, 26*(103), 85–100.

Creswell, J. W. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, CA: SAGE.

Darmadi, N. S. (2015). Kritik penyelenggaraan sistem jaminan sosial nasional di Indonesia. *Jurnal Pembaharuan Hukum, 2*(2).

Denzin, N. K., & Lincoln, Y. S. (2017). *The SAGE handbook of qualitative research*. Thousand Oaks, CA: SAGE Publications.

du Cluzel, F. (2021). *Cognitive warfare: The future of cognitive dominance*. NATO Innovation Hub.

Fairclough, N. (2015). *Language and power* (3rd ed.). London: Routledge.

Foucault, M. (1978). *The history of sexuality* (Vol. 1: An introduction). New York, NY: Pantheon Books.

Freedman, L. (2019). *Strategy: A history*. Oxford, UK: Oxford University Press.

Giles, K. (2022). *Moscow Rules: What drives Russia to confront the West*. Washington, DC: Brookings Institution Press.
Haryono, D. (2022). *Pertahanan siber Indonesia: Tantangan dan arah kebijakan nasional*. Jakarta: LIPI Press.
Helmus, T. C. (2018). *Russian social media influence*. Santa Monica, CA: RAND Corporation.
Horton, B. (2021). This is not propaganda: Adventures in the war against reality. *International Affairs, 97*(1). https://doi.org/10.1093/ia/iiaa208
Karim, M. (2018). Mahalnya keteladanan Pancasila. *Jurnal Kesejahteraan Sosial, 1*(2). https://doi.org/10.31326/jks.v1i02.146
Laksmana, E. (2020). The end of "hedging"? Indonesia's China policy and the South China Sea. *Asia Policy, 15*(1), 116–123.
Lanoszka, A. (2020). Disinformation in international politics. *European Journal of International Security, 5*(2), 227–250.
Mankoff, J. (2021). *Russian influence operations in the digital age*. Washington, DC: Center for Strategic and International Studies (CSIS).
Nye, J. S. (2018). *The future of power*. New York, NY: PublicAffairs.
Nye, J. S. (2021). Soft power and global politics in the digital era. *Foreign Affairs Review, 99*(4), 12–25.
Pomerantsev, P. (2019). *This is not propaganda: Adventures in the war against reality*. London: Faber & Faber.
Rattray, G. J. (2020). *Strategic warfare in cyberspace: Cognitive dimensions and national security*. Cambridge, MA: MIT Press.
Shuvalova, M. (2020). This is not propaganda: Adventures in the war against reality by Peter Pomerantsev. *Kyiv-Mohyla Humanities Journal, 7*. https://doi.org/10.18523/kmhj219687.2020-7.263-265
Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Boston, MA: Houghton Mifflin Harcourt.
Thomas, T. (2018). Russia's reflexive control theory and the nature of information warfare. *Journal of Slavic Military Studies, 31*(4), 331–353.
Toffler, A., & Toffler, H. (1993). *War and anti-war: Survival at the dawn of the 21st century*. New York, NY: Little, Brown and Company.
Triolo, P., & Allison, K. (2018). *The Digital Silk Road: China's new global strategy* (Eurasia Group Report).
Tzu, S. (2010). *The art of war* (R. Sawyer, Trans.). New York, NY: Basic Books.
U.S. Department of Defense. (2023). *Summary of the 2023 Department of Defense cyber strategy*. Washington, DC: U.S. Department of Defense.