



Kepemimpinan Digital dan Tata Kelola Siber sebagai Landasan Reformulasi Doktrin Pertahanan Nasional Indonesia dalam Perspektif Rusia Amerika Serikat dan Israel

Wis Yudha, Wirasetyo Haprabu, Tarsisius Susilo, Taufiq Zega, Didik Purwanto

Sesko TNI, Indonesia.

Email: yudhabonaparte@gmail.com, pipinghot.id@gmail.com, muchsus70@gmail.com,
mtaufiqzega13@gmail.com, halilintar1997@gmail.com

ABSTRAK

Kata kunci:

pertahanan siber,
kepemimpinan digital, tata
kelola siber, reformulasi
doktrin, kedaulatan digital.

Transformasi digital global telah mendefinisikan ulang lanskap pertahanan nasional, di mana kekuatan siber menjadi elemen strategis kedaulatan negara. Penelitian ini menganalisis model kepemimpinan digital dan tata kelola siber dalam doktrin pertahanan Rusia, Amerika Serikat, dan Israel, serta relevansinya bagi reformulasi doktrin pertahanan nasional Indonesia. Menggunakan pendekatan kualitatif dengan metode studi kebijakan dan analisis komparatif, penelitian ini mengkaji dokumen kebijakan, publikasi resmi pemerintah, dan literatur akademis terkait pertahanan siber. Hasil penelitian menunjukkan bahwa Rusia mengembangkan model kepemimpinan digital terpusat berbasis information warfare, Amerika Serikat menerapkan pendekatan kolaboratif dengan doktrin defend forward, sementara Israel membangun ekosistem pertahanan inovatif melalui integrasi militer-industri-akademik. Analisis terhadap posisi Indonesia mengungkapkan kesenjangan antara kesiapan normatif dan kapabilitas operasional, dengan tantangan utama berupa fragmentasi kelembagaan dan ketiadaan doktrin pertahanan siber terpadu. Berdasarkan temuan tersebut, penelitian ini merekomendasikan model sintesis yang mengintegrasikan disiplin strategis ala Rusia, interoperabilitas kelembagaan ala Amerika Serikat, dan kecepatan inovasi ala Israel, yang disesuaikan dengan nilai-nilai Pancasila dan sistem pertahanan semesta. Implementasi model ini melalui pembentukan Komando Pertahanan Siber Nasional, penyusunan Undang-Undang Pertahanan Siber, dan pengembangan ekosistem pembelajaran siber diharapkan dapat memperkuat kedaulatan digital Indonesia dalam menghadapi ancaman siber global.

Kepemimpinan Digital Dan Tata Kelola Siber Sebagai Landasan Reformulasi Doktrin Pertahanan Nasional Indonesia Dalam Perspektif Rusia Amerika Serikat Dan Israel

Keywords: *cyber defense, digital leadership, cyber governance, doctrine reformulation, digital sovereignty*

Abstract

Global digital transformation has redefined the national defense landscape, where cyber power is a strategic element of state sovereignty. This study analyzes the digital leadership and cyber governance models in the defense doctrines of Russia, the United States, and Israel, as well as their relevance to the reformulation of Indonesia's national defense doctrine. Using a qualitative approach with policy study methods and comparative analysis, this study examines policy documents, official government publications, and academic literature related to cyber defense. The results show that Russia is developing a centralized digital leadership model based on information warfare, the United States is implementing a collaborative approach with the defend forward doctrine, while Israel is building an innovative defense ecosystem through military-industry-academic integration. An analysis of Indonesia's position reveals a gap between normative readiness and operational capability, with the main challenges being institutional fragmentation and the absence of an integrated cyber defense doctrine. Based on these findings, this study recommends a synthesis model that integrates Russian-style strategic disciplines, United States-style institutional interoperability, and Israeli-style innovation speeds, which are adjusted to the values of Pancasila and the universal defense system. The implementation of this model through the establishment of the National Cyber Defense Command, the drafting of the Cyber Defense Law, and the development of a cyber learning ecosystem is expected to strengthen Indonesia's digital sovereignty in the face of global cyber threats.

PENDAHULUAN

Transformasi digital global telah mengubah lanskap pertahanan nasional dari orientasi kekuatan fisik menuju dominasi information power yang berbasis data, algoritma, dan jaringan siber. Dalam konteks geopolitik modern, kekuatan digital tidak hanya menjadi elemen penunjang, tetapi telah berfungsi sebagai instrumen strategis kedaulatan nasional dan alat proyeksi kekuasaan global (Nye, 2018). Rusia, Amerika Serikat, dan Israel adalah tiga negara yang berhasil menampilkan pola kepemimpinan digital dan tata kelola siber yang terinstitusionalisasi dalam doktrin pertahanan nasionalnya, yakni masing-masing dengan model, struktur, dan filosofi keamanan yang berbeda namun saling beririsan dalam tujuan strategis menjaga supremasi digital nasional (Cavelty, 2018; Giles, 2016; Healey, 2019). Rusia mengembangkan sistem pertahanan siber berbasis information warfare yang dikendalikan negara secara sentralistik melalui doktrin *Gerasimov Doctrine*, menekankan fusi antara operasi siber, psikologis, dan propaganda digital sebagai bagian dari strategi nasional (Galeotti, 2016). Amerika Serikat membangun U.S. Cyber Command (USCYBERCOM) sebagai entitas kepemimpinan siber nasional dengan konsep *defend forward* dan *persistent engagement* untuk

Kepemimpinan Digital Dan Tata Kelola Siber Sebagai Landasan Reformulasi Doktrin Pertahanan Nasional Indonesia Dalam Perspektif Rusia Amerika Serikat Dan Israel

mengantisipasi ancaman sebelum mencapai infrastruktur vital (Nakasone & Lewis, 2021). Sementara Israel menampilkan model yang paling inovatif melalui integrasi sektor pertahanan, industri teknologi, dan akademisi di bawah ekosistem Unit 8200, yang secara strategis memadukan kepemimpinan digital dengan pengembangan inovasi pertahanan (Singer & Friedman, 2014).

Indonesia berada dalam fase strategis untuk mengkonsolidasikan doktrin pertahanan nasional berbasis digital yang mampu menjawab ancaman multidimensi di era siber. Berdasarkan *Global Cybersecurity Index 2021* yang diterbitkan oleh ITU, Indonesia menempati posisi ke-24 dunia, jauh di bawah Amerika Serikat (peringkat 1), Rusia (peringkat 5), dan Israel (peringkat 6) (ITU, 2021). Sementara itu, laporan Badan Siber dan Sandi Negara (BSSN, 2023) mencatat terdapat lebih dari 1,6 miliar serangan siber sepanjang tahun 2022 yang sebagian besar menargetkan infrastruktur strategis, termasuk sistem pertahanan dan pemerintahan. Fakta ini menunjukkan adanya kesenjangan signifikan antara kompleksitas ancaman dan kesiapan institusional pertahanan digital nasional. Secara normatif, arah pembangunan pertahanan nasional di era digital telah ditegaskan dalam Peraturan Presiden Nomor 68 Tahun 2024 tentang Rencana Pembangunan Jangka Menengah Nasional (RPJMN) 2025–2029, yang menetapkan “Transformasi Digital untuk Kedaulatan Nasional” sebagai agenda prioritas strategis negara. Dokumen tersebut menekankan pentingnya integrasi sistem pertahanan siber nasional, penguatan tata kelola digital lintas kelembagaan, dan peningkatan kapasitas sumber daya manusia pertahanan yang adaptif terhadap perubahan teknologi global (Bappenas, 2024). Selain itu, Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara masih menjadi kerangka yuridis utama yang mengamanatkan penyelenggaraan pertahanan secara semesta dengan melibatkan seluruh sumber daya nasional, termasuk teknologi dan informasi. Dalam konteks ini, das sollen-nya adalah bahwa Indonesia harus memiliki doktrin pertahanan siber nasional yang menjadi instrumen ideologis, strategis, dan operasional dalam menghadapi ancaman siber transnasional secara terukur dan terarah (Nye, 2011; Perwita & Setiawan, 2021).

Namun dalam realitas empiris, sistem pertahanan Indonesia masih berorientasi pada ancaman konvensional dan belum sepenuhnya mengadopsi paradigma kepemimpinan digital serta tata kelola siber yang terpadu. Fragmentasi kelembagaan antara Kementerian Pertahanan, BSSN, dan TNI mengakibatkan tidak adanya satu kerangka komando siber nasional yang memiliki mandat strategis tunggal. Penelitian Lembaga Ilmu Pengetahuan Indonesia (LIPI, 2022) menunjukkan bahwa hingga kini belum terdapat doktrin pertahanan nasional yang mengintegrasikan dimensi *cyber deterrence*, *information dominance*, dan *digital resilience* secara komprehensif. Kondisi tersebut melahirkan beberapa persoalan mendasar yang menjadi fokus kajian ini, yaitu: 1) Bagaimana model kepemimpinan digital dan tata kelola siber diterapkan oleh Rusia, Amerika Serikat, dan Israel dalam membangun kekuatan pertahanan nasional di era digital, serta bagaimana praktik tersebut dapat dijadikan acuan bagi Indonesia dalam membangun arsitektur pertahanan siber yang strategis; 2) Bagaimana posisi dan kesiapan Indonesia dalam mengintegrasikan kepemimpinan digital dan tata kelola siber ke dalam reformulasi doktrin pertahanan nasional, terutama dalam konteks kebijakan, sumber daya manusia, dan infrastruktur teknologi; dan 3) Bagaimana model konseptual reformulasi doktrin

pertahanan nasional Indonesia yang adaptif terhadap dinamika ancaman siber global dan kompatibel dengan arah kebijakan RPJMN 2025–2029 menuju kedaulatan digital nasional. Ketiga rumusan masalah tersebut secara substansial berangkat dari kesenjangan empiris antara *das sollen* (tuntutan normatif negara terhadap modernisasi pertahanan digital) dan *das sein* (realitas faktual keterbatasan tata kelola siber nasional), sehingga diperlukan formulasi konseptual baru yang mampu menjembatani kedua dimensi tersebut melalui pendekatan kepemimpinan digital yang adaptif dan teknokratik.

Studi-studi sebelumnya telah mengidentifikasi keberhasilan ketiga negara tersebut dalam membangun ketahanan siber. Penelitian oleh Tabrizi & Gheytsi (2022) dalam *Journal of Strategic Security* mengonfirmasi bahwa efektivitas kepemimpinan digital bergantung pada integrasi visi strategis dengan kapasitas teknis dan budaya organisasi. Sementara itu, kajian Lembaga Ilmu Pengetahuan Indonesia (LIPI, 2022) mengungkapkan bahwa Indonesia masih menghadapi fragmentasi kelembagaan antara Kementerian Pertahanan, BSSN, dan TNI, serta belum adanya doktrin pertahanan siber terpadu. Namun, penelitian terdahulu belum secara komprehensif menganalisis bagaimana model kepemimpinan digital dan tata kelola siber dari ketiga negara rujukan dapat diadaptasi ke dalam konteks Indonesia yang berlandaskan nilai-nilai Pancasila dan sistem pertahanan semesta. Kesenjangan inilah yang menjadi fokus penelitian ini, dengan menawarkan kebaruan melalui sintesis model hibrida yang memadukan disiplin strategis ala Rusia, interoperabilitas kelembagaan ala Amerika Serikat, dan kecepatan inovasi ala Israel, yang disesuaikan dengan karakteristik ideologis dan kelembagaan Indonesia.

Penulisan jurnal ini menjadi penting secara akademis, strategis, dan praktis karena berupaya menghadirkan perspektif baru dalam disiplin ilmu pertahanan Indonesia, yakni integrasi antara kepemimpinan digital, tata kelola siber, dan reformulasi doktrin pertahanan nasional dalam kerangka sistem pertahanan adaptif. Secara spesifik, penelitian ini bertujuan untuk: (1) menganalisis model kepemimpinan digital dan tata kelola siber dalam doktrin pertahanan Rusia, Amerika Serikat, dan Israel; (2) mengevaluasi kesiapan Indonesia dalam mengintegrasikan dimensi digital ke dalam doktrin pertahanan nasional; serta (3) merumuskan model sintesis yang adaptif dengan nilai-nilai Pancasila dan sistem pertahanan semesta. Kajian ini juga memberikan kontribusi nyata bagi penguatan basis konseptual kebijakan publik pertahanan di Indonesia yang selama ini masih berorientasi konvensional. Dengan mengadopsi pengalaman Rusia, Amerika Serikat, dan Israel, artikel ini berupaya memberikan model sintesis yang sesuai dengan konteks ideologi dan sistem pertahanan semesta Indonesia. Secara teknokratik, hasil penelitian ini diharapkan dapat menjadi referensi strategis bagi pembuat kebijakan di Kementerian Pertahanan, TNI, dan BSSN dalam merumuskan doktrin pertahanan siber nasional yang visioner, interoperabel, dan berkarakter Pancasila sebagai wujud transformasi pertahanan Indonesia menuju kedaulatan digital dan daya tangkal strategis abad ke-21.

METODE PENELITIAN

Penelitian ini menggunakan metode survei deskriptif (Moleong, 2019). Metode survei deskriptif merupakan pendekatan yang digunakan untuk memperoleh data melalui penyebaran angket atau kuesioner kepada responden yang telah ditentukan sebelumnya. Dalam penelitian ini, data diperoleh dari delapan orang responden berusia antara 17 hingga

45 tahun, yang terdiri atas empat laki-laki dan empat perempuan dari berbagai jenjang pendidikan. Survei ini bertujuan untuk menggambarkan pandangan masyarakat mengenai isu toleransi dan relevansi nilai-nilai Pancasila dalam kehidupan berbangsa.

Pertanyaan dalam survei terdiri atas tiga butir utama, yaitu: (1) seberapa penting nilai toleransi dalam kehidupan berbangsa; (2) apakah nilai-nilai Pancasila masih relevan dalam menyikapi tindakan intoleransi; dan (3) apakah responden pernah menyaksikan tindakan intoleransi. Data yang diperoleh kemudian dianalisis secara deskriptif guna mengidentifikasi pola pemahaman serta persepsi responden terhadap pentingnya nilai-nilai toleransi dan Pancasila dalam menjaga kerukunan di tengah keberagaman masyarakat Indonesia (Sunaryati et al., 2023; Syalsabiluna et al., 2023).

HASIL DAN PEMBAHASAN

Bagian pembahasan ini diarahkan untuk menganalisis hasil identifikasi masalah yang telah diuraikan sebelumnya secara sistematis dan kritis. Analisis difokuskan pada bagaimana dinamika kepemimpinan digital dan tata kelola siber berpengaruh terhadap kebutuhan reformulasi doktrin pertahanan nasional Indonesia, khususnya dalam konteks ketertinggalan adaptasi strategis terhadap perubahan lingkungan keamanan global. Pembahasan ini menempatkan identifikasi masalah bukan sekadar sebagai daftar persoalan, tetapi sebagai dasar analitis untuk menguji kesenjangan konseptual dan empiris antara norma kebijakan yang diharapkan dan realitas pelaksanaannya. Melalui pendekatan komparatif terhadap model Rusia, Amerika Serikat, dan Israel, bagian ini bertujuan menguraikan bagaimana masing-masing negara mengembangkan sistem kepemimpinan siber, struktur tata kelola, serta arsitektur doktrin pertahanan digital yang terintegrasi. Secara teknokratik, pembahasan ini berfungsi untuk menilai posisi strategis Indonesia dalam kerangka global, sekaligus mengidentifikasi komponen kunci yang perlu diadaptasi untuk membangun doktrin pertahanan siber nasional yang responsif, berdaya tangkal, dan berbasis kemandirian teknologi

Model kepemimpinan digital dan tata kelola siber diterapkan oleh Rusia, Amerika Serikat, dan Israel dalam membangun kekuatan pertahanan nasional di era digital

Dalam arsitektur kekuasaan kontemporer, ranah siber telah berubah dari sekadar medium komunikasi menjadi domain strategis yang menentukan distribusi kekuatan, efektivitas pencegahan, dan legitimasi kedaulatan. Pergeseran ini menuntut konfigurasi kepemimpinan digital yang bukan hanya memahami teknologi, melainkan mampu menyusun tata kelola lintas-institusi yang koheren, menginternalisasi logika risiko, dan menautkan inovasi dengan doktrin pertahanan yang dapat diuji di lapangan. Kerangka teoretik *smart power* dan *cyber power* Joseph Nye membantu menjelaskan bahwa dominasi di era digital lahir dari kemampuan menggabungkan daya paksa, legitimasi normatif, dan orkestrasi informasi dalam satu ekosistem kebijakan yang konsisten (Nye, 2018). Sementara itu, transformational leadership memberi prasyarat kultural dan organisasional (yakni visi, inspirasi, dan perubahan sistem) yang membuat teknologi bermakna strategis alih-alih sekadar artefak. Di atas fondasi ini, Rusia, Amerika Serikat, dan Israel menampilkan tiga arketipe kepemimpinan siber yang sama-sama efektif tetapi berbeda orientasi, yaitu sentralisasi koersif dengan kontrol informasi,

interoperabilitas institusional dengan proyeksi ofensif, dan ekosistem inovasi yang dikurasi negara namun digerakkan pasar.

Rusia mengonstruksi kepemimpinan digitalnya dalam bingkai non-linear warfare, di mana batas damai-perang diregangkan melalui operasi informasi, psikologi, dan siber yang saling menguatkan. Tafsir paling berpengaruh atas “*Gerasimov Doctrine*” (lebih sebagai meta-narasi praktik ketimbang naskah operasional) menunjukkan bahwa Moskow memosisikan ruang siber sebagai vektor pengaruh yang menyatu dengan diplomasi koersif dan operasi penggalangan (Galeotti, 2016). Secara kelembagaan, komando berada pada struktur negara keamanan yang vertikal; koordinasi antara Kementerian Pertahanan, GRU, dan FSB membentuk rantai keputusan yang pendek untuk operasi intrusi, influence, hingga disruption. Hukum *Sovereign Internet* mempertebal digital *sovereignty* Rusia dengan opsi isolasi jaringan nasional yang memberikan keunggulan defensif dalam skenario decoupling dan kebalikan arus informasi (Rid, 2020). Dari sudut teori organisasi, ini adalah machine bureaucracy yang efisien pada mobilisasi cepat, tetapi membayar harga pada derajat exploration inovasi terbuka, yaitu sebuah *trade-off* klasik antara kecepatan komando dan keragaman solusi (Mintzberg, 2017). Namun tidak berarti inovasi absen; yang terjadi adalah inovasi terkurasi yang diarahkan pada spektrum *active measures* dan *information confrontation* alih-alih inovasi produk komersial. Dampak operasional terlihat pada kampanye disinformation dan hack-and-leak lintas teater yang menyasar proses politik dan infrastruktur sipil lawan, memadukan *plausible deniability* dan *cost-imposition* di bawah ambang eskalasi konvensional (Rid, 2020). Kritik utama peneliti pada model ini ialah risiko *blowback* reputasional dan biaya jangka panjang terhadap ekosistem inovasi domestik, yaitu sentralisasi memperkuat disiplin strategi, tetapi berpotensi menumpulkan learning loop yang membutuhkan umpan balik lintas komunitas teknis independen.

Amerika Serikat menempuh jalan berbeda dengan membangun kepemimpinan digital berbasis *network governance* dan *whole-of-government approach*. Elevasi USCYBERCOM ke *unified combatant command* menandai reposisi siber dari dukungan teknis menjadi domain operasi penuh, sementara konsep defend forward/persistent engagement mereformulasi defensif tradisional menjadi *contest in contact*, yaitu mengganggu lawan di hulu, sebelum mencapai infrastruktur kritis domestik (Nakasone & Lewis, 2021). Hal ini menuntut integrasi NSA, DoD, DHS/CISA, komunitas intelijen, dan sektor swasta kritis, yang dalam teori *adaptive leadership* memerlukan kapasitas mengelola konflik nilai, ketidakpastian, dan pembelajaran cepat pada batas organisasi. Keunggulan model AS bukan semata anggaran dan teknologi, tetapi *interoperability by design*, yaitu standar, playbook bersama, simulasi lintas-matra, dan mekanisme berbagi intelijen ancaman yang relatif institutionalized (CSIS, 2021). Insiden besar seperti *Stuxnet*, *NotPetya*, dan *SolarWinds* menjadi *stress test* yang mendorong pergeseran ke arsitektur *zero trust*, peningkatan *supply-chain security*, dan investasi pada *hunt forward ops*, yakni serangkaian intervensi yang memperlihatkan bagaimana krisis diubah menjadi agenda perubahan teknis dan regulatif (CSIS, 2021). Secara kultural, Schein mengingatkan bahwa keberhasilan transformasi butuh *embedding mechanisms*, yaitu apa yang diukur, diberi penghargaan, dan ditoleransi (Schein, 2010). Ketika metrik seperti MTTD/MTTR, kepatuhan zero trust, dan frekuensi *red-teaming* menjadi KPI lintas instansi, maka kepemimpinan digital tidak beroperasi pada retorika, melainkan pada disiplin operasional

yang dapat diaudit. Kelemahan bawaan model ini adalah kompleksitas koordinasi dan fragmentasi mandat yang rentan politisasi; namun, *mekanisme oversight* dan *checks-and-balances* justru menciptakan *resilience by redundancy*, jika satu katup gagal, katup lain menutup celah.

Israel memadukan kedua dunia (disiplin strategis negara dan dinamika inovasi pasar) ke dalam model yang dapat disebut *networked transformational leadership*. INCD bertindak sebagai otak kebijakan dan risk orchestrator, sementara Unit 8200 berperan sebagai *talent engine* dan *innovation flywheel* yang menghidupi ekosistem *start-up nation* di domain keamanan digital (Singer & Friedman, 2014). Kekuatan sejati model ini bukan sekadar kecakapan teknis, melainkan *learning architecture* yang memfasilitasi siklus ide dari operasi militer ke pasar, lalu kembali ke militer sebagai kapabilitas yang diperkaya pengalaman lapangan, yakni persis prinsip *learning organization* Senge tentang feedback loops dan systems thinking. Negara bertindak sebagai *curator* (bukan *command-and-control* penuh) dengan memberi ruang eksperimen, *challenge-driven procurement*, dan akses pasar internasional melalui diplomasi keamanan. Hasilnya adalah *time-to-capability* yang cepat, yaitu solusi sensorik, kriptografi, dan *AI-for-cyber* yang dapat beradaptasi terhadap skenario lawan yang berubah cepat. Secara normatif, ada kritik mengenai *civil-military fusion* dan etika ekspor teknologi intrusif; namun dari lensa pertahanan murni, koherensi antara pengindraan ancaman, bakat teknis, dan inovasi terapan membuat Israel unggul pada *precision cyber effects* dan *intelligence fusion*, sesuatu yang sukar ditandingi oleh birokrasi yang kaku.

Membandingkan ketiganya memerlukan lensa yang menyatukan struktur, budaya, dan strategi. Castells menyatakan kekuasaan di era jaringan bergantung pada kemampuan menata arus informasi dan node strategis; Rusia menguasai arus melalui kontrol, Amerika melalui standar dan koalisi, Israel melalui ekosistem dan kecepatan pembelajaran. Dalam kerangka Bass & Riggio, Rusia menonjol pada *idealized influence* terpusat, AS pada intellectual stimulation institusional, dan Israel pada individualized consideration terhadap talenta yang disalurkan ke misi nasional. Mintzberg membantu memetakan bentuk organisasional, dimana Rusia condong ke *machine bureaucracy* yang sinkron untuk operasi spektrum pengaruh; AS menggabungkan professional *bureaucracy* dan *divisionalized* form yang memberi spesialisasi dan skalabilitas; Israel mendekati *adhocracy* yang unggul dalam inovasi dan respons (Mintzberg, 2017). Tidak ada *one best way*; ada fit terhadap ancaman, budaya politik, dan tujuan strategis. Namun, jika tujuan adalah daya tangkal jangka panjang, peneliti berargumen bahwa model yang menyeimbangkan disiplin komando dengan varian inovasi (sebagaimana nuansa Israel) memberi option value lebih besar di bawah ketidakpastian teknologi.

Dari perspektif efektivitas operasional, kedewasaan kepemimpinan digital dalam pertahanan tidak dapat diukur melalui frekuensi serangan yang berhasil digagalkan ataupun jumlah operasi yang dinyatakan “sukses,” melainkan melalui kemampuan sistemik untuk menutup celah kerentanan, memulihkan layanan kritikal dalam waktu minimal, dan mempertahankan strategic narrative di tengah disrupsi yang kompleks. Kepemimpinan digital yang matang ditandai bukan oleh kecepatan reaksi semata, tetapi oleh konsistensi respons

strategis yang mampu menjaga legitimasi, stabilitas sistemik, dan kesinambungan operasi lintas domain bahkan ketika terjadi penetrasi signifikan.

Amerika Serikat menjadi contoh paradigmatik dalam membangun model kepemimpinan berbasis pembelajaran krisis. Pasca insiden SolarWinds, AS tidak sekadar memperbaiki sistem keamanan teknisnya, melainkan mengubah kerangka pikir pertahanan digital secara menyeluruh: dari pendekatan perimeter-centric menuju identitas dan rantai pasok sebagai pusat gravitasi keamanan nasional. Transformasi menuju federal zero trust architecture dan penerapan *software bill of materials* (SBOM) menunjukkan pergeseran dari paradigma reaktif ke paradigma antisipatif, yang menekankan traceability, transparansi, dan risk-based orchestration lintas lembaga (CSIS, 2021).

Sebaliknya, Rusia menampilkan model kepemimpinan siber yang berkarakter strategic opportunism, yakni memadukan *plausible deniability*, operasi *information warfare*, dan *cost-imposition* di bawah ambang perang terbuka. Pendekatan ini terbukti efektif dalam mengendalikan domain “abu-abu” geopolitik, menciptakan efek deterensi melalui kebingungan strategis lawan, namun menimbulkan konsekuensi jangka menengah berupa tekanan isolasi teknologi dan menurunnya kapasitas penyerapan inovasi global (*absorptive capacity*) akibat *decoupling* ekonomi-politik yang berkepanjangan (Rid, 2020).

Israel, di sisi lain, menonjol dalam integrasi intelijen pra-serangan (*left-of-boom intelligence*) dengan operasi presisi digital yang disinergikan bersama langkah *kinetic de-escalation*, menghasilkan kemampuan unik dalam menjaga eskalasi tetap terkendali sambil mempertahankan *reputational deterrence* yang kredibel di mata regional maupun global. Pendekatan ini menunjukkan bahwa kepemimpinan digital yang efektif bukan hanya mampu mengelola teknologi, tetapi juga mampu menyusun koherensi antara strategi informasi, efek militer, dan legitimasi diplomatik.

Dari komparasi tersebut dapat disimpulkan bahwa pendekatan persistent engagement Amerika Serikat dan knowledge loop Israel menawarkan pola kepemimpinan yang lebih berkelanjutan dalam ekosistem teknologi yang hiper-dinamis dan penuh disrupsi. Model ini menumbuhkan kemampuan belajar adaptif (*adaptive learning capability*) dan ketahanan institusional terhadap ketidakpastian. Sebaliknya, *commandism* ala Rusia, meskipun unggul dalam efektivitas operasi jangka pendek dan kampanye yang menuntut koordinasi naratif terpusat, berisiko membatasi inovasi serta menciptakan ketergantungan pada kontrol hierarkis yang sulit beradaptasi terhadap kompleksitas ancaman siber modern. Dengan demikian, efektivitas operasional kepemimpinan digital tidak semata diukur dari keberhasilan menangkis serangan, tetapi dari kemampuan mentransformasikan krisis menjadi pengetahuan, pengetahuan menjadi kebijakan, dan kebijakan menjadi ketahanan strategis nasional yang berkelanjutan.

Secara kebijakan, tata kelola siber yang menopang kepemimpinan digital mesti mengikat tiga lapis, yaitu kerangka hukum yang jelas, mekanisme koordinasi yang dapat diuji, dan metrik kinerja yang berorientasi hasil. Rusia memaku lapis pertama dengan regulasi kedaulatan digital dan kontrol platform; koordinasi berlangsung melalui aparaturnya keamanan negara, dan metrik keberhasilan lebih sulit diaudit publik karena sifatnya tertutup. AS, dengan tradisi *oversight*, mengikat lapis pertama melalui mandat legislatif, lapis kedua melalui lembaga seperti CISA sebagai national risk manager, dan lapis ketiga melalui indikator teknis serta asesmen

independen (CSIS, 2021). Israel menggunakan pendekatan hibrida: hukum sebagai pagar, INCD sebagai orchestrator, dan pasar sebagai akselerator metrik keberhasilan, dimana *time-to-deploy* dan efektivitas operasional menjadi indikator utama. Argumen peneliti: tata kelola yang memadukan *compliance* dan *capability* akan menghindari jebakan “seremonial kepatuhan” yang menghasilkan dokumen tanpa daya tangkal. Karena itu, indikator seperti MTTD/MTTR insiden kritis, tingkat adopsi multi-factor authentication dan least privilege, serta frekuensi uji red-team nasional seharusnya menjadi bahasa bersama antaraktor.

Dengan demikian, hakikat keberhasilan kepemimpinan digital dalam pertahanan modern tidak diukur dari seberapa banyak sumber daya manusia dimobilisasi, melainkan dari sejauh mana kepemimpinan mampu mengonversi talent menjadi *capability*, dan *capability* menjadi *deterrence* yang kredibel dan berkelanjutan. Kepemimpinan digital yang efektif bukan sekadar menciptakan kompetensi individual, tetapi mentransformasikan potensi manusia menjadi sistem kemampuan nasional yang terorganisasi, terukur, dan mampu menghasilkan efek strategis yang konsisten lintas domain. Rusia menunjukkan bahwa disiplin komando informasi dan kontrol terpusat dapat mengekstraksi kemampuan secara presisi, menghasilkan respons terkoordinasi yang efisien dalam operasi kampanye. Amerika Serikat, sebaliknya, mengubah kapabilitas menjadi kekuatan melalui skala dan interoperabilitas lintas-lembaga, menciptakan ecosystem deterrence yang bergantung pada sinergi sistem, bukan pada satu pusat otoritas. Sedangkan Israel mengilustrasikan bentuk kepemimpinan digital yang paling dinamis, yakni memperpendek jarak antara inovasi, pengujian, dan penerapan melalui siklus pembelajaran cepat (*innovation-deployment cycle*) dan orientasi misi yang kuat, di mana setiap krisis menjadi laboratorium strategis bagi pembaruan doktrin dan alat pertahanan.

Peneliti berpendapat bahwa garis kausal utama yang membedakan ketiganya terletak pada variabel “*learning velocity*”, yaitu kemampuan ekosistem nasional (negara, militer, industri, dan academia) untuk mendeteksi perubahan taktis, mengekstraksi pelajaran operasional, dan mengkodifikasikannya ke dalam doktrin serta sistem pertahanan yang hidup. Semakin cepat suatu bangsa belajar, semakin kuat daya tangkal strategisnya. Namun, *learning velocity* hanya dapat muncul apabila mekanisme pembelajaran dijalankan dalam keseimbangan antara arah komando dan ruang otonomi inovasi. Teori organisasi pembelajar menunjukkan bahwa transformasi digital akan macet ketika struktur kepemimpinan hanya bersifat instruktif tanpa kapasitas reflektif. Dalam kondisi demikian, teknologi hanya menjadi simbol modernisasi, bukan instrumen pembelajaran kolektif.

Dalam konteks ini, Israel menawarkan pelajaran paling signifikan tentang bagaimana budaya organisasi pertahanan dapat menjadi inkubator inovasi tanpa kehilangan disiplin militer; Amerika Serikat menunjukkan bagaimana sistem demokratis mampu mengubah kompleksitas birokrasi menjadi ketangguhan adaptif; sedangkan Rusia menjadi peringatan konseptual bahwa kontrol total memang menjamin presisi kampanye, tetapi berisiko menghambat asimilasi ide, kolaborasi partisipatif, dan inovasi lintas domain yang justru menjadi inti keunggulan jangka panjang. Oleh karena itu, kepemimpinan digital di masa depan harus menyeimbangkan tiga kekuatan besar (disiplin strategis, kapasitas koordinatif, dan kelincahan belajar) agar doktrin pertahanan tidak berhenti sebagai produk kebijakan, melainkan

berevolusi menjadi sistem pembelajaran nasional yang terus memperbarui dirinya seiring dinamika ancaman global.

Artinya, ketiga model menawarkan *design pattern* yang dapat diambil secara selektif: disiplin komando naratif dan *unity of effort* Rusia, *persistent engagement* dan *institutional interoperability* Amerika Serikat, serta *ecosystemic learning* dan *challenge-driven innovation* Israel. Kombinasi ketiganya, jika ditata dengan kejelasan mandat, metrik berbasis hasil, dan *talent pipeline* yang berkelanjutan, akan menghasilkan kepemimpinan digital yang tidak hanya responsif, tetapi juga proaktif, adaptif, dan memiliki *deterrence credibility* di mata kawan dan lawan. Dalam tatanan siber seiring dengan perkembangan global saat ini, keunggulan tidak lagi ditentukan oleh satu lompatan teknologi, melainkan oleh konsistensi kepemimpinan yang menegakkan tata kelola, mengukur kemajuan dengan jujur, dan mempercepat putaran belajar kebangsaan.

Posisi dan kesiapan Indonesia dalam mengintegrasikan kepemimpinan digital dan tata kelola siber ke dalam reformulasi doktrin pertahanan nasional.

Posisi Indonesia dalam arsitektur pertahanan digital nasional saat ini dapat dipahami sebagai fase transisi paradigmatis, yakni pergeseran gradual dari sistem pertahanan konvensional yang berorientasi pada kekuatan fisik dan platform militer menuju paradigma informasi yang terintegrasi, adaptif, dan berbasis jaringan. Fase transisi ini menandai perubahan mendasar dalam cara negara memandang kekuatan pertahanan, yakni bukan lagi semata sebagai kemampuan kinetik, tetapi sebagai kapasitas kognitif, digital, dan organisasional untuk mengelola risiko, mengintegrasikan teknologi, serta mengantisipasi ancaman multidimensi di domain siber.

Di satu sisi, arah pembangunan nasional sebagaimana tertuang dalam RPJMN 2025–2029 telah menempatkan transformasi digital sebagai agenda strategis lintas-sektor yang memadukan pembangunan ekonomi, keamanan, dan kedaulatan teknologi. Paradigma ini menegaskan bahwa pertahanan digital bukan sekadar domain teknis, melainkan *strategic enabler* bagi ketahanan nasional secara keseluruhan. Namun di sisi lain, kesiapan kelembagaan pertahanan (mulai dari Kemhan, TNI, hingga BSSN) masih menghadapi tantangan fragmentasi otoritas dan ketidaksinambungan visi strategis. Kondisi tersebut menyebabkan konsep *unity of effort* di ranah pertahanan digital belum sepenuhnya terwujud; koordinasi antar-lembaga sering kali bersifat ad hoc, prosedural, dan tidak menghasilkan *interoperability of effect* yang diperlukan dalam konteks ancaman siber lintas domain.

Dalam kerangka tersebut, kepemimpinan digital di sektor pertahanan Indonesia masih cenderung normatif dan belum sepenuhnya bertransformasi menjadi kapabilitas institusional yang terukur. Banyak kebijakan strategis berhenti pada tataran wacana tanpa didukung arsitektur pelaksanaan, pengukuran kinerja, dan budaya organisasi yang memungkinkan inovasi berlangsung secara berkelanjutan. Ketegangan antara ambisi strategis (membangun kedaulatan digital nasional) dan realitas implementatif (keterbatasan struktur, SDM, dan tata kelola) inilah yang menjadi poros utama analisis kesiapan pertahanan digital Indonesia.

Pertanyaan fundamentalnya bukan lagi apakah Indonesia siap secara normatif, melainkan sejauh mana negara ini mampu mengembangkan dan mengonsolidasikan kapasitas kepemimpinan digital (visi strategis, mandat kelembagaan, struktur koordinasi, dan budaya

organisasi) serta tata kelola siber (regulasi, proses, metrik, dan mekanisme pengawasan) yang dapat diinternalisasi ke dalam doktrin pertahanan nasional yang benar-benar adaptif, terukur, dan dapat diuji melalui indikator kinerja lintas domain.

Dalam konteks ini, tantangan Indonesia tidak terletak pada kekurangan strategi, melainkan pada defisit integrasi dan keberlanjutan kebijakan. Reformulasi doktrin pertahanan digital harus berperan sebagai bridging framework, yaitu yang menjembatani jurang antara visi dan eksekusi, antara kebijakan dan teknologi, antara komando dan pembelajaran. Hanya dengan menjadikan kepemimpinan digital sebagai fungsi strategis yang melekat dalam tata kelola pertahanan, Indonesia dapat memastikan bahwa transformasi digital tidak berhenti sebagai slogan modernisasi, tetapi menjadi proses institusional yang mengubah cara negara berpikir, bertindak, dan bertahan dalam ekosistem ancaman siber global (Nye, 2018).

Secara konseptual, kepemimpinan digital pertahanan menuntut tiga kualitas simultan: kemampuan menyusun visi yang dapat dieksekusi, kemampuan mengkoordinasikan jaringan aktor yang heterogen, dan kemampuan menutup execution gap antara kebijakan dan operasi. Teori *transformational leadership* menekankan bahwa perubahan sistemik mensyaratkan idealized influence dan intellectual stimulation yang menggerakkan organisasi untuk belajar dan berinovasi melampaui kebiasaan lama. Dalam konteks pertahanan siber, kualitas ini diterjemahkan menjadi pengarusutamaan standar teknis (misalnya kerangka NIST CSF), pemutakhiran arsitektur ke *zero trust*, penguatan *threat intelligence* bersama, dan pengukuran kinerja berbasis metrik operasional seperti MTDD/MTTR, *patch latency*, dan *mean time to recover*, yakni serangkaian praktik yang hanya berjalan apabila kepemimpinan digital memiliki mandat jelas dan legitimasi lintas-lembaga (CSIS, 2021; Schein, 2010).

Di tingkat tata kelola, Indonesia telah memiliki elemen-elemen kunci (regulasi dasar pertahanan, lembaga siber nasional, kerangka pembangunan digital, dan program peningkatan talenta) namun konsolidasi menjadi command architecture yang utuh masih belum tuntas. Fragmentasi mandat antara regulator siber nasional, perencana kebijakan pertahanan, dan operator militer menghasilkan tumpang tindih kewenangan dalam pencegahan, deteksi, respons, dan pemulihan insiden. Dari kacamata *network governance*, masalahnya bukan sekadar “siapa memimpin,” melainkan “bagaimana orkestrasi risiko dilakukan” sehingga setiap aktor mengetahui perannya, indikator capaian bersama, serta *protokol handover* dalam skenario eskalasi dari insiden sipil ke ancaman pertahanan. Tanpa orkestrasi itu, investasi teknologi sering berubah menjadi *technology theatre* yakni tampak canggih, tetapi tidak memperbaiki ketahanan sistemik.

Fakta ancaman mengonfirmasi urgensi tersebut, misalnya mengacu kepada hasil Laporan tahunan BSSN merekam lonjakan insiden dan anomali lalu lintas berbahaya yang menyasar sektor pemerintahan dan infrastruktur vital, yaitu indikasi bahwa *attack surface* nasional melebar sejalan dengan digitalisasi layanan publik dan rantai pasok (BSSN, 2023). Indeks keamanan siber global menempatkan Indonesia pada kelompok “menengah-atas,” namun jarak terhadap *front-runners* masih nyata, terutama pada aspek kesiapsiagaan operasional, *supply-chain assurance*, dan *cross-sector exercises* berskala nasional (ITU, 2021). Data dan indeks ini tidak dimaknai sebagai vonis, melainkan sebagai leading indicators yang menuntut reposisi

kebijakan: dari orientasi “*compliance and projects*” menuju “*capability and outcomes*”, yaitu sebuah pergantian logika dari menghitung jumlah program ke mengukur kecepatan deteksi dan ketahanan layanan kritikal.

Kesiapan sumber daya manusia menjadi variabel pembeda. Tantangan Indonesia bukan hanya soal jumlah perwira dan analis siber, tetapi skill mix yang sesuai dengan operasi gabungan digital, yakni *reverse engineering*, *intelijen siber*, *threat hunting*, *forensik*, *operasi ofensif defensif* terintegrasi, hingga *campaign assessment*. Teori *learning organization* menunjukkan bahwa organisasi yang sanggup merotasi pembelajaran lintas fungsi (doktrin, operasi, riset, dan akuisisi) akan memperpendek jarak antara pengetahuan dan kemampuan. Pada titik inilah praktik negara perbandingan memberi pelajaran, yaitu kemampuan untuk mematri *talent pipeline* yang mengalir dari pendidikan tinggi ke unit operasi dan kembali ke pusat inovasi menentukan “kecepatan belajar nasional,” sebuah metrik yang sering tak terlihat tetapi menentukan *deterrence credibility*. Indonesia telah memulai berbagai inisiatif talenta digital dan *cyber range* pelatihan; tantangannya adalah memastikan loop antara latihan teknis, *evaluasi red team/blue team*, dan perbaikan doktrin tidak terputus oleh siklus anggaran dan rotasi personel.

Dari sisi arsitektur teknis, sebagian besar lingkungan pemerintah bergerak ke arah implementasi zero trust dan penguatan identitas, namun adaptasi pada tingkat mission systems pertahanan memerlukan standar yang lebih ketat, pengendalian integritas perangkat keras/lunak (SBOM, *secure boot*, *device attestation*), serta integrasi threat intel yang dapat dieksekusi langsung ke kebijakan *endpoint* dan *network microsegmentation* (CSIS, 2021). Kesiapan di sini bukan sekadar ketersediaan alat, melainkan keterpaduan *policy-to-control plane* yang memungkinkan *rollback* cepat, karantina otomatis, dan *deception ops* pada jaringan misi. Doktrin baru harus mengafirmasi bahwa desain teknis adalah kebijakan yang dibekukan dalam kode (*policy as code*) sehingga kepemimpinan digital dapat mengatur laju adaptasi melalui parameter yang diaudit, bukan memo yang terlambat (Nye, 2018; Schein, 2010).

Kesenjangan utama yang perlu dijembatani doktrin adalah transisi dari “pembagian tugas administratif” menuju “komando efek terpadu.” Pada praktiknya, spektrum insiden siber jarang berhenti di batas yurisdiksi; ia bergerak dari probing ke *credential theft*, menembus rantai pasok, dan menyasar sistem *operational technology* yang menopang layanan publik dan dukungan logistik pertahanan. Karena itu, doktrin pertahanan siber Indonesia yang direformulasi harus menetapkan jalur eskalasi yang jelas dari *civil cyber incident* ke *national defense contingency*, lengkap dengan kriteria pengambilalihan komando, *rules of engagement*, dan *legal carve-outs* untuk operasi *hunt forward* yang sah dan proporsional (CSIS, 2021). Kesiapan saat ini mengindikasikan adanya protokol koordinasi, tetapi standarisasi *playbook* gabungan, *table-top exercise* lintas sektor yang rutin, dan evaluasi *pasca-insiden* yang menagih perbaikan sistemik masih perlu diperdalam agar *learning loop* menghasilkan perubahan yang terukur.

Budaya organisasi adalah sumbu keberhasilan atau kegagalan. Schein menegaskan bahwa budaya berubah ketika pemimpin mengubah apa yang diukur, dihargai, dan ditoleransi (Schein, 2010). Jika kegagalan audit keamanan tidak menimbulkan konsekuensi, sementara inovasi yang berisiko justru dihukum, organisasi akan memilih status quo yang aman namun rapuh. Kepemimpinan digital pertahanan Indonesia karenanya harus secara sadar menata ulang

mekanisme penghargaan dan sanksi: keberhasilan bukan hanya “tiada insiden besar,” tetapi “peningkatan kecepatan deteksi, kualitas respons, dan ketahanan layanan.” Indikator inilah yang perlu ditarik masuk ke dashboard pemimpin politik-militer sehingga tata kelola siber menjadi bahasa pengambilan keputusan, bukan jargon teknis di ruang server.

Aspek hukum dan legitimasi publik tidak kalah penting. Operasi siber yang efektif sering memerlukan tindakan pra-emptif, perburuan aktif di jaringan mitra, atau manipulasi *infrastructure as code* yang menyentuh wilayah abu-abu hukum. Tanpa kerangka legal yang jelas dan mekanisme oversight yang kredibel, kapabilitas teknis berisiko menurunkan legitimasi politik dan dukungan publik. Model negara demokratis menunjukkan bahwa legitimasi dibangun dengan *bounded discretion*, yakni ruang manuver operasi diberikan, namun diikat akuntabilitas, audit, dan pelaporan berjadwal kepada lembaga pengawas (CSIS, 2021). Kesiapan Indonesia pada domain ini akan menentukan apakah doktrin baru mampu bertahan melewati siklus politik, sebab keberlanjutan (bukan hanya keunggulan sesaat) adalah sumber deterensi di era siber (Nye, 2018).

Dari perspektif strategi, kesiapan terbaik lahir dari kombinasi hardening jangka pendek, integrasi menengah, dan adaptasi jangka panjang. Dalam jangka pendek, celah prioritas pada identitas, akses istimewa, dan perangkat rantai pasok harus ditutup dengan disiplin teknis dan *patch governance* yang ketat. Pada horizon menengah, pembentukan komando dan pusat operasi siber gabungan (dengan antarmuka reguler ke BSSN, kepolisian siber, dan operator infrastruktur vital) perlu diinstitusionalisasi, termasuk *fusion center* intelijen siber yang menghasilkan *indicators and warnings* yang dapat dieksekusi oleh satuan misi. Pada horizon panjang, ekosistem inovasi pertahanan-sipil-akademik harus dipacu melalui challenge-driven procurement, bug bounty nasional untuk infrastruktur kritis, dan test ranges terpadu untuk OT/IT, yaitu menciptakan *learning velocity* yang menjadi keunggulan komparatif. Kesiapan Indonesia saat ini telah menginjakkan kaki pada tahap pertama, namun percepatan ke tahap kedua dan ketiga menuntut keputusan doktrinal yang berani: menjadikan kepemimpinan digital sebagai mesin perubahan yang mengikat strategi, struktur, proses, dan budaya.

Artinya bahwa **fit doktrin pertahanan siber Indonesia idealnya bersifat hibrida**, yakni disiplin komando untuk memastikan *unity of effort* pada krisis; interoperabilitas institusional untuk daya lenting dan skala; serta ekosistem inovasi untuk kecepatan belajar dan keberlanjutan. Pelajaran dari negara pembanding (seperti Rusia, AS dan Israel) menunjukkan bahwa mengandalkan satu dimensi saja tidak cukup. Sentralisasi murni menambah ketangkasan komando namun mengerdilkan kreativitas; desentralisasi murni merangsang inovasi namun rentan *coordination failure*. Karena itu, reformulasi doktrin harus *men-design modular centralization*, yaitu komando terpadu untuk efek, namun antarmuka modular untuk inovasi dan dukungan industri, sehingga jalur dari ide ke kemampuan dan dari kemampuan ke deterensi menjadi pendek dan berulang (Mintzberg, 2017).

Pada tataran pengukuran, kesiapan pertahanan digital tidak seharusnya dipahami secara administratif, melainkan harus ditentukan oleh *time-bound outcomes* yang dapat diverifikasi secara empiris. Doktrin pertahanan siber yang baru perlu bergeser dari orientasi “kepatuhan terhadap dokumen” menuju paradigma *governance by performance*, di mana setiap kebijakan

dievaluasi berdasarkan capaian kuantitatif yang terukur, konsisten, dan berorientasi hasil. Target kinerja tersebut harus meliputi penurunan *Mean Time to Detect* (MTTD) dan *Mean Time to Recover* (MTTR) secara tahunan, peningkatan tingkat adopsi multi-factor authentication hingga mencapai 100% di seluruh lingkungan infrastruktur kritikal, perluasan cakupan *real-time asset inventory* untuk memastikan visibilitas sistem nasional secara menyeluruh, percepatan durasi pemulihan layanan kritikal dalam skenario simulasi krisis nasional, serta peningkatan frekuensi *joint cyber exercises* lintas sektor sebagai indikator koordinasi antar-lembaga. Melalui sistem pengukuran berbasis hasil tersebut, kepemimpinan digital pertahanan akan memiliki *strategic dashboard* yang secara langsung menghubungkan keputusan kebijakan dengan kinerja teknis, menjadikan tata kelola siber bukan lagi simbol retorik, melainkan kontrak kinerja yang transparan, dapat diaudit, dan memiliki akuntabilitas lintas-level kelembagaan (Schein, 2010; CSIS, 2021).

Dengan demikian, posisi Indonesia dalam evolusi pertahanan digital dapat dipetakan sebagai “siap secara konseptual, berkembang secara kelembagaan, dan menanjak secara operasional.” Namun, kematangan sistemik tersebut mensyaratkan keberanian politik dan kelembagaan untuk mengikat kepemimpinan digital ke dalam doktrin yang secara serempak mengatur struktur komando, standar teknis, mekanisme pembelajaran, serta metrik kinerja lintas domain. Dalam kerangka ini, kesiapan tidak lagi dipandang sebagai kondisi statis yang dicapai sekali waktu, melainkan sebagai laju pembelajaran nasional (*the rate of learning*), yaitu seberapa cepat bangsa mengonversi pengalaman menjadi aturan, aturan menjadi kode, dan kode menjadi ketahanan yang berlapis. Bila reformulasi doktrin pertahanan mampu memikul fungsi penghela ini, maka Indonesia tidak sekadar mengejar ketertinggalan dari negara rujukan seperti Rusia, Amerika Serikat, dan Israel, tetapi mampu membangun *deterrence credibility* yang berakar pada kemandirian teknologi, legitimasi publik, dan budaya keselamatan digital yang melembaga, yakni sebuah fondasi strategis bagi kedaulatan nasional di era informasi yang saling terkoneksi.

Model konseptual reformulasi doktrin pertahanan nasional Indonesia yang adaptif terhadap ancaman siber global berdasarkan pembelajaran dari Rusia, Amerika Serikat, dan Israel.

Dalam lanskap keamanan global, ruang siber telah berevolusi menjadi domain strategis kelima setelah darat, laut, udara, dan luar angkasa. Perubahan ini menuntut setiap negara untuk menata ulang cara pandangnya terhadap kekuatan nasional, karena dominasi militer kini tidak lagi ditentukan semata oleh kemampuan senjata, tetapi oleh penguasaan terhadap informasi, teknologi, dan kecepatan adaptasi digital (Nye, 2018). Indonesia, dengan sistem pertahanan semestanya yang berlandaskan Pancasila, menghadapi tantangan baru, yaitu bagaimana mengintegrasikan kepemimpinan digital dan tata kelola siber ke dalam doktrin pertahanan yang selama ini didesain untuk menghadapi ancaman konvensional. Reformulasi ini tidak cukup hanya berupa pembaruan terminologi, tetapi harus berupa rekayasa paradigma, yakni pergeseran dari *defense as reaction* menuju *defense as anticipation*.

Pelajaran penting dapat diambil dari tiga negara utama yaitu Rusia, Amerika Serikat, dan Israel, yakni tiga model dengan karakter yang kontras namun saling melengkapi. Rusia menampilkan model kepemimpinan siber terpusat yang menempatkan kontrol negara atas arus

informasi sebagai sumber kekuasaan strategis. Di bawah doktrin *information warfare*, Rusia menggunakan operasi siber, psikologis, dan diplomatik secara simultan untuk membentuk persepsi dan menciptakan keunggulan geopolitik (Galeotti, 2016). Kekuatan model ini terletak pada kemampuannya menciptakan *unity of effort* (kesatuan tujuan dan arah) yang memastikan semua elemen negara bekerja dalam kerangka narasi nasional yang tunggal. Namun, kelemahannya juga jelas: sentralisasi ekstrem menumpulkan inovasi, memperlambat adaptasi terhadap teknologi baru, dan menciptakan ketergantungan pada birokrasi yang tertutup (Rid, 2020). Dengan kata lain, Rusia unggul dalam kecepatan mobilisasi, tetapi rentan kehilangan fleksibilitas.

Sebaliknya, Amerika Serikat mengembangkan model kepemimpinan siber kolaboratif yang bersifat *multi-level governance*. Melalui doktrin *defend forward* dan *persistent engagement*, AS berupaya tidak hanya mempertahankan diri dari serangan, tetapi secara aktif menekan lawan di wilayah sibernya sendiri (Nakasone & Lewis, 2021). Model ini berpijak pada prinsip interoperabilitas, yaitu menggabungkan kekuatan lembaga militer, sipil, dan industri teknologi dalam satu sistem koordinasi nasional. US *Cyber Command* (USCYBERCOM) berperan sebagai pengendali utama operasi siber pertahanan, sementara lembaga seperti CISA dan NSA berperan dalam pencegahan dan respons sipil. Kelebihan pendekatan ini adalah kemampuannya menciptakan *deterrence through engagement*, di mana ancaman dihadapi bukan setelah terjadi, tetapi dicegah di hulu. Namun, model ini juga menghadapi kompleksitas koordinasi antarlembaga yang kadang menyebabkan *policy lag* antara keputusan strategis dan pelaksanaan teknis (CSIS, 2021).

Israel menjadi contoh paling dinamis dalam memadukan kepemimpinan siber dan inovasi nasional. Negara ini berhasil membangun ekosistem *military-industry-academia* yang terhubung dalam siklus pembelajaran berkelanjutan (Singer & Friedman, 2014). Unit 8200 berfungsi bukan hanya sebagai satuan intelijen siber, tetapi juga sebagai inkubator teknologi nasional. Model Israel menempatkan keamanan digital sebagai motor ekonomi dan sumber daya strategis bangsa, bukan beban anggaran militer semata. Kelebihannya terletak pada kecepatan inovasi (*learning velocity*) dan fleksibilitas adaptasi, dua hal yang menjadikan Israel mampu bertahan menghadapi ancaman siber yang terus berevolusi. Namun, tantangan etis dan keamanan tetap mengintai, terutama dalam menjaga keseimbangan antara kepentingan pertahanan dan privasi sipil.

Belajar dari Rusia, Amerika Serikat, dan Israel, jelas bahwa pertahanan siber bukan hanya perkara perangkat keras atau firewall, tetapi merupakan hasil dari sistem yang mampu memimpin, mengelola, belajar, dan beradaptasi secara terus-menerus. Rusia unggul dalam sentralisasi visi strategis dan narasi kebangsaan; Amerika Serikat menonjol dalam koordinasi multi-level antar lembaga dan interoperabilitas hukum-teknis; sedangkan Israel menjadi contoh keberhasilan integrasi inovasi militer dan sipil dalam satu ekosistem digital yang lincah dan produktif (Galeotti, 2016; Nakasone & Lewis, 2021; Singer & Friedman, 2014).

Bagi Indonesia, tantangan terbesar bukan sekadar mengadopsi model luar, tetapi menemukan sintesis antara karakter nasional (yakni pertahanan semesta berbasis Pancasila) dengan tata kelola digital yang terukur, terbuka, dan berdaya tangkal tinggi. Maka, delapan

konsep berikut disusun sebagai kerangka konseptual komprehensif untuk membentuk doktrin pertahanan siber nasional yang adaptif, integratif, dan berkelanjutan. Reformulasi doktrin yang adaptif terhadap ancaman siber global berarti menempatkan ruang digital sebagai domain utama yang memiliki struktur komando, mekanisme operasi, indikator kinerja, dan siklus pembelajaran tersendiri. Doktrin baru tidak lagi berhenti pada norma umum “melindungi kedaulatan negara di dunia maya,” tetapi harus menetapkan *who commands, how to respond, what to measure, dan how to learn*. Dengan demikian, pertahanan siber tidak lagi reaktif, melainkan proaktif, terukur, dan berkelanjutan.

Dua Analisis diatas juga menunjukkan bahwa keberhasilan reformulasi doktrin tidak dapat dilepaskan dari budaya organisasi yang mendukung transparansi, akuntabilitas, dan evaluasi berbasis hasil. Menurut Schein (2010), budaya organisasi berubah ketika pemimpin mengubah apa yang diukur dan dihargai. Oleh karena itu, indikator doktrin harus konkret, misalnya tingkat keberhasilan deteksi ancaman, waktu pemulihan infrastruktur kritikal, dan kecepatan konversi hasil insiden menjadi kebijakan baru. Hanya dengan cara itu, doktrin pertahanan siber Indonesia dapat menjadi dokumen hidup, bukan sekadar panduan statis. Adapun konseptual reformulasi doktrin pertahanan nasional Indonesia yang adaptif terhadap ancaman siber global, antara lain:

a. Konsep Kedaulatan Digital (*Digital Sovereignty Doctrine*).

Kedaulatan digital adalah fondasi normatif utama doktrin pertahanan siber Indonesia. Konsep ini menegaskan bahwa kemandirian pertahanan tidak dapat dipisahkan dari penguasaan atas data nasional, algoritma, dan infrastruktur kritikal negara. Dalam model Rusia, kedaulatan digital diwujudkan melalui *Sovereign Internet Law* (2019) yang memungkinkan isolasi jaringan nasional ketika krisis (Rid, 2020). Indonesia dapat mengambil pelajaran dari pendekatan ini tanpa mengimitasi kontrol total: kedaulatan digital Indonesia harus berbasis regulasi, interoperabilitas, dan transparansi publik. Dalam konteks Pancasila, kedaulatan digital bukan berarti isolasi, melainkan kemampuan mengatur dan melindungi ruang digital nasional tanpa kehilangan keterhubungan global.

b. Konsep Kepemimpinan Digital Transformasional (*Transformational Digital Leadership*).

Kepemimpinan pertahanan di era digital tidak lagi hanya soal komando hierarkis, tetapi kemampuan mengintegrasikan visi strategis dengan adaptasi teknologi dan budaya organisasi. Pemimpin pertahanan digital harus menjadi digital statesman, yakni figur yang mampu menghubungkan dimensi teknis, ideologis, dan etis dalam pengambilan keputusan siber. Model Rusia menekankan *centralized strategic discipline*; model AS memperlihatkan *multi-level distributed leadership*; dan Israel memperagakan *networked mission leadership*. Indonesia perlu mengembangkan kepemimpinan digital adaptif: kombinasi ketegasan arah (Rusia), kapasitas koordinatif (AS), dan kelincahan inovatif (Israel).

c. Konsep Tata Kelola Siber Terpadu (*Integrated Cyber Governance*).

Tata kelola siber yang efektif harus melampaui koordinasi sektoral dan menjadi mekanisme komando lintas-lembaga. Dalam model AS, USCYBERCOM memimpin operasi militer sementara CISA dan NSA menjaga aspek sipil dan intelijen (Nakasone & Lewis, 2021). Indonesia membutuhkan arsitektur serupa yang disesuaikan dengan struktur Sistem Pertahanan Semesta. Konsep Komando Pertahanan Siber Nasional (Kopsibnas) dapat dijadikan simpul

pengendali strategis, bekerja sejajar dengan BSSN dan Ditjen Strahan Kemhan. Prinsipnya yaitu *unity of command* dalam krisis, *unity of effort* dalam kesiapsiagaan.

d. Konsep Ekosistem Pembelajaran Siber Nasional (*National Cyber Learning Ecosystem*).

Pelajaran paling kuat dari Israel adalah bahwa keunggulan siber berasal dari kecepatan belajar institusional. Setiap insiden diolah menjadi pembelajaran yang memperkaya doktrin, pelatihan, dan inovasi teknologi (Singer & Friedman, 2014; Senge, 1990). Indonesia harus membangun *National Cyber Learning Ecosystem* yang menghubungkan militer, academia, industri, dan komunitas digital. Ekosistem ini menciptakan “*learning loop*” nasional (meliputi insiden-analisis-inovasi-revisi doktrin). Dengan demikian, pertahanan siber Indonesia menjadi sistem hidup yang berevolusi bersama ancaman.

e. Konsep Ketahanan Adaptif dan Interoperabilitas (*Adaptive Resilience and Interoperability*).

Konsep ini menuntut doktrin yang fleksibel, bukan kaku pada skenario tertentu. Model AS menunjukkan efektivitas *defend forward* dan *persistent engagement*, yakni strategi yang menekankan deteksi dan tindakan dini di luar batas yurisdiksi (CSIS, 2021). Indonesia dapat menerapkannya melalui mekanisme kerja sama regional dan protokol joint incident response. Doktrin adaptif harus menjamin interoperabilitas sistem antara Kemhan–TNI–BSSN–Polri, baik dalam arsitektur data, komunikasi, maupun latihan gabungan. Ketahanan tidak lagi diukur dari “tidak diserang,” melainkan seberapa cepat sistem pulih dan belajar setelah serangan (Schein, 2010).

f. Konsep Kemandirian Teknologi Pertahanan (*Defense Tech Sovereignty*).

Kemandirian teknologi adalah elemen tak terpisahkan dari kedaulatan siber. Indonesia harus memiliki strategi selective self-reliance, yakni mandiri pada komponen krusial seperti kriptografi, *root-of-trust hardware*, sistem identitas nasional, dan sensor pertahanan digital, sembari tetap terhubung ke ekosistem inovasi global (Nye, 2018). Israel menjadi contoh sukses, yakni melalui kombinasi investasi negara dan kolaborasi industri, teknologi sibernya tidak hanya melindungi tetapi juga menghasilkan nilai ekonomi strategis. Indonesia dapat meniru pola ini dengan *defense innovation hub* yang memadukan riset militer dan sipil di bawah Kemhan.

g. Konsep Komando Efek Siber dan Hukum Eskalasi (*Cyber Effects Command and Escalation Law*).

Salah satu kelemahan besar banyak negara adalah absennya pedoman hukum jelas untuk operasi offensive cyber. Model AS menunjukkan pentingnya *rules of engagement* (ROE) dan otoritas penggunaan daya siber yang jelas (CSIS, 2021). Indonesia perlu memasukkan dimensi ini ke dalam doktrin baru: menentukan kriteria eskalasi dari insiden sipil menuju ancaman pertahanan nasional, siapa yang berwenang mengambil keputusan, serta batas legal operasi *hunt forward* dan *active defense*. Dengan demikian, ruang abu-abu hukum siber bisa diatur secara etis dan proporsional.

h. Konsep Narasi Strategis Pertahanan Digital (*Digital Strategic Narrative*).

Pertahanan di era informasi tidak hanya dimenangkan dengan kekuatan senjata, tetapi juga dengan penguasaan narasi (Rid, 2020). Rusia memanfaatkan information warfare untuk

mempengaruhi opini publik global, sementara AS menggunakan *strategic communication* berbasis fakta dan koalisi internasional. Indonesia harus membangun narasi pertahanan digital yang mencerminkan karakter nasional, yaitu pertahanan rakyat semesta di ruang digital. Narasi ini tidak bersifat koersif, melainkan inspiratif: mengajak masyarakat menjadi bagian dari ketahanan siber nasional, memperkuat *cyber patriotism* berbasis nilai-nilai Pancasila.

i. Sistem Deterrence Digital Nasional (*National Digital Deterrence System*).

Deterrence tidak lagi diukur hanya dengan jumlah senjata, melainkan oleh kredibilitas kemampuan siber negara. Indonesia perlu membangun *Cyber Deterrence Index* (CDI), yakni indikator nasional untuk mengukur kesiapan digital pertahanan. CDI mencakup lima metrik utama: (1) kemampuan deteksi dini, (2) kecepatan pemulihan, (3) tingkat adopsi teknologi pertahanan digital, (4) ketahanan rantai pasok, dan (5) kapasitas SDM pertahanan digital (Nye, 2018). Indeks ini berfungsi sebagai alat ukur kebijakan dan diplomasi strategis.

j. Infrastruktur Kritis dan Proteksi Berlapis (*Layered Critical Infrastructure Defense*).

Doktrin baru harus menetapkan *layered defense approach*:

- 1) Layer 1 (*Preventive Layer*), yaitu pencegahan serangan dengan enkripsi dan segmentasi jaringan,
- 2) Layer 2 (*Detective Layer*), yaitu sistem pemantauan terintegrasi (SIEM, SOAR),
- 3) Layer 3 (*Reactive Layer*), yaitu tim respons insiden cepat,
- 4) Layer 4 (*Recovery Layer*), yaitu pemulihan otomatisasi sistem dan pelaporan real-time.

k. Kolaborasi Siber Regional dan Diplomasi Pertahanan (*Regional Cyber Collaboration & Cyber Diplomacy*).

Sebagai negara kunci di Indo-Pasifik, Indonesia harus membangun *Cyber Defense Cooperation Framework* dengan negara ASEAN, Australia, Jepang, dan Korea Selatan. Doktrin baru perlu menempatkan diplomasi siber sebagai bagian dari smart defense Indonesia, mengikuti model koalisi siber Amerika dan sekutu NATO (Nye, 2018). Kerja sama regional memungkinkan latihan bersama, berbagi ancaman, dan interoperabilitas pertahanan digital kawasan.

Kesimpulan

Transformasi digital global telah menggeser esensi pertahanan nasional dari dominasi kekuatan fisik menuju supremasi data, informasi, dan kecerdasan buatan. Dalam konteks ini, reformulasi doktrin pertahanan Indonesia menjadi keniscayaan strategis untuk memastikan kedaulatan negara di tengah konvergensi ancaman siber, disinformasi, dan perang informasi lintas domain. Pembelajaran dari Rusia, Amerika Serikat, dan Israel memperlihatkan bahwa keunggulan pertahanan digital lahir dari keseimbangan antara sentralisasi arah strategis, koordinasi lintas-lembaga, dan inovasi terbuka yang berkelanjutan. Indonesia, meski telah memiliki kerangka kebijakan digital dalam RPJMN 2025–2029, masih menghadapi kesenjangan antara ambisi strategis dan kesiapan operasional, terutama pada aspek kepemimpinan digital, tata kelola siber terpadu, dan penguasaan teknologi pertahanan. Reformulasi doktrin pertahanan nasional Indonesia yang adaptif terhadap ancaman siber global harus menempatkan kepemimpinan digital sebagai pusat gravitasi, tata kelola siber sebagai instrumen pengendali, dan ekosistem pembelajaran nasional sebagai sumber daya

regeneratif. Doktrin baru tidak cukup bersifat deklaratif, tetapi harus menjadi policy engine yang menggerakkan struktur komando, arsitektur teknologi, dan budaya organisasi pertahanan digital yang berbasis data, disiplin, dan pembelajaran berkelanjutan. Dengan demikian, pertahanan siber Indonesia tidak hanya bersifat defensif, tetapi juga mampu menciptakan strategic deterrence yang kredibel serta memastikan kedaulatan digital sebagai bagian integral dari ketahanan nasional yang modern dan berkarakter Pancasila. Oleh sebab itu, Pemerintah Indonesia perlu segera membentuk Komando Pertahanan Siber Nasional sebagai simpul kendali lintas-matra TNI, menetapkan Undang-Undang Pertahanan Siber Nasional yang mengatur kewenangan dan mekanisme eskalasi ancaman digital, serta membangun Pusat Fusi Siber Nasional untuk integrasi data intelijen dan respons insiden. Selain itu, penguatan ekosistem pembelajaran dan inovasi pertahanan digital perlu dipercepat melalui pendirian *Cyber Defense Academy*, *Defense Innovation Hub*, dan *Cyber Sandbox* Nasional yang menghubungkan militer, academia, dan industri. Tanpa langkah-langkah konkret tersebut, reformulasi doktrin pertahanan Indonesia akan berhenti pada tataran konseptual; dengan langkah tersebut, Indonesia justru dapat memimpin arah keamanan digital kawasan Indo-Pasifik dengan kekuatan pertahanan yang berdaulat, terukur, dan berorientasi masa depan.

DAFTAR PUSTAKA

- Badan Perencanaan Pembangunan Nasional. (2024). Rencana Pembangunan Jangka Menengah Nasional (RPJMN) 2025–2029. Jakarta: Bappenas.
- Badan Siber dan Sandi Negara. (2023). Laporan Tahunan Keamanan Siber Nasional 2022. Jakarta: BSSN.
- BSSN. (2023). Laporan Tahunan Keamanan Siber Nasional 2022. Badan Siber dan Sandi Negara.
- Cavelty, M. D. (2018). Cybersecurity in Switzerland: Between complexity, cooperation and controversy. *Swiss Political Science Review*, 24(1), 35–43.
- Creswell, J. W. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Los Angeles: SAGE Publications.
- CSIS. (2021). *Defending forward in cyberspace: Strategy and implementation*. Center for Strategic and International Studies.
- Galeotti, M. (2016). *The Gerasimov Doctrine and Russian non-linear war*. Moscow: Institute for International Studies.
- Giles, K. (2016). Russia's 'new' tools for confronting the West: Continuity and innovation in Moscow's exercise of power. Chatham House Research Paper.
- Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, 5(1), 1–15.
- International Telecommunication Union. (2021). *Global Cybersecurity Index 2021*. Geneva: ITU.
- Lembaga Ilmu Pengetahuan Indonesia. (2022). *Kajian kesiapan pertahanan siber nasional*. Jakarta: Pusat Kajian Keamanan Nasional.

- Mintzberg, H. (2017). *Managing the myths of health care (konsep bentuk organisasi diadaptasi lintas-sektor)*. San Francisco: Berrett-Koehler.
- Moleong, L. J. (2019). *Metodologi penelitian kualitatif*. Bandung: PT Remaja Rosdakarya.
- Nakasone, P., & Lewis, J. (2021). *Defending forward and persistent engagement in cyberspace*. Washington, D.C.: CSIS.
- Nye, J. S. (2011). *The future of power*. New York: PublicAffairs.
- Nye, J. S. (2018). *The future of power in the digital age*. Oxford: Oxford University Press.
- Perwita, A. A. B., & Setiawan, R. (2021). Cyber defense strategy in Indonesia: Challenges and opportunities in the digital era. *Indonesian Journal of International Relations*, 5(2), 178–195.
- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. New York: Farrar, Straus and Giroux.
- Schein, E. H. (2010). *Organizational culture and leadership (4th ed.)*. San Francisco: Jossey-Bass.
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. New York: Oxford University Press.