

## KEPEMIMPINAN RUSIA, AMERIKA SERIKAT, DAN ISRAEL DALAM PENGELOLAAN SUMBER DAYA SIBER SEBAGAI PEMBELAJARAN BAGI DOKTRIN PERTAHANAN SIBER INDONESIA

**Eko Syah Putra Siregar, Amin Bagiono, Tarsisius Susilo, Bungkus Hadisuseno, Cahyadi Amperawan.**

Sekolah Staf dan Komando TNI

Email: syahpu53@gmail.com, amin.bagiono@gmail.com, muchsus70@gmail.com, b.hadisusenoseno@gmail.com dan Anakunikah@gmail.com

### Abstract

*The rapid advancement of digital technology has reshaped the global defense landscape, positioning cyberspace as a new strategic domain in the competition for national power. Countries such as Russia, the United States, and Israel demonstrate distinct leadership models in managing digital resources and developing resilient cyber defense systems. This study aims to analyze the characteristics of strategic leadership in these three nations and identify relevant lessons for the formulation of Indonesia's cyber defense doctrine, characterized by national values and aligned with the vision of Indonesia Emas 2045. The research employs a qualitative descriptive method using a policy analysis approach through literature review and examination of official documents from defense institutions and international strategic studies. The findings reveal that the United States exhibits transformational and collaborative leadership, Russia demonstrates firm and centralized strategic-military leadership, while Israel reflects adaptive and innovative leadership driven by technological research. The synthesis of these models suggests that Indonesia's cyber defense doctrine should integrate the values of Pancasila, strengthen cross-sector leadership among government, military, and technology industries, and promote defense research innovation to reinforce digital sovereignty and enhance national cyber resilience in the digital era.*

**Keyword:** Amerika Serikat, Cyber, Israel, Rusia.

### Abstrak

Perkembangan teknologi digital telah mengubah paradigma pertahanan global, menempatkan ruang siber sebagai domain strategis baru dalam kompetisi kekuatan nasional. Negara-negara seperti Rusia, Amerika Serikat, dan Israel menampilkan pola kepemimpinan yang berbeda dalam mengelola sumber daya digital serta membangun sistem pertahanan siber yang tangguh dan adaptif. Penelitian ini bertujuan untuk menganalisis karakteristik kepemimpinan strategis

ketiga negara tersebut serta mengidentifikasi pembelajaran yang relevan bagi pengembangan doktrin pertahanan siber Indonesia yang berkarakter nasional dan berorientasi pada visi Indonesia Emas 2045. Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan analisis kebijakan (*policy analysis*) melalui telaah literatur dan dokumen resmi dari lembaga pertahanan dan kajian strategis internasional. Hasil penelitian menunjukkan bahwa Amerika Serikat menonjol dalam kepemimpinan transformasional dan kolaboratif, Rusia menunjukkan kepemimpinan strategis-militer yang tegas dan terpusat, sedangkan Israel menampilkan kepemimpinan adaptif dan inovatif berbasis riset teknologi pertahanan. Sintesis dari ketiga model tersebut merekomendasikan perlunya Indonesia membangun doktrin pertahanan siber yang berlandaskan nilai-nilai Pancasila, memperkuat kepemimpinan lintas-sektor antara pemerintah, militer, dan industri teknologi, serta mengembangkan inovasi riset pertahanan untuk memperkuat kedaulatan digital dan meningkatkan daya tangkal nasional di era siber.

**Kata Kunci:** *Amerika Serikat, Israel, Rusia, Siber.*

Diserahkan: 03-09-2025; Diterima: 10-10-2025; Diterbitkan: 20-10-2025

## PENDAHULUAN

Perkembangan teknologi digital telah mengubah karakter ancaman keamanan global dari yang bersifat konvensional menjadi multidomain, di mana ruang siber kini menjadi arena strategis baru dalam kompetisi kekuatan antarnegara. Fenomena ini menunjukkan bahwa dimensi pertahanan tidak lagi terbatas pada aspek militer, melainkan meluas hingga ranah informasi, ekonomi, sosial, dan psikologis. Serangan siber terhadap infrastruktur kritis, manipulasi informasi publik, serta infiltrasi sistem komando dan kendali militer menjadi instrumen baru dalam upaya melemahkan kedaulatan suatu negara tanpa konfrontasi fisik langsung (Adma, 2023). Dalam konteks pertahanan modern, kemampuan suatu negara dalam mengelola sumber daya digital, membangun sistem keamanan siber nasional, serta mengintegrasikan kebijakan lintas-sektor mencerminkan tingkat kesiapan dan efektivitas kepemimpinan strategis nasional dalam menghadapi ancaman hybrid dan disinformasi global (N. R. A. dkk., 2025).

Amerika Serikat merupakan pelopor dalam integrasi kebijakan keamanan siber nasional. Melalui *National Cybersecurity Strategy*, AS mengadopsi pendekatan *whole-of-nation* yang menekankan redistribusi tanggung jawab keamanan digital dari individu ke lembaga yang memiliki kapasitas mitigasi risiko sistemik (The White House, 2023). Pendekatan ini menandai perubahan paradigma keamanan dari yang bersifat reaktif menjadi proaktif, dengan fokus pada pembangunan sistem pertahanan siber yang resilien dan terintegrasi. Strategi tersebut diperkuat oleh *Department of Defense (DoD) Cyber Strategy*, yang menekankan konsep *persistent engagement* dan *defend forward* sebagai langkah pencegahan terhadap potensi serangan siber terhadap aset strategis nasional (U.S. Department of Defense, 2023). Pola kepemimpinan transformasional dan kolaboratif ini

menunjukkan bagaimana visi politik dan strategi pertahanan digital dapat disinergikan dalam satu kerangka kebijakan nasional yang komprehensif.

Sebaliknya, Israel menonjol dengan model kepemimpinan siber berbasis inovasi dan koordinasi lintas-sektor. Melalui pembentukan *Israel National Cyber Directorate (INCD)*, negara ini mengembangkan mekanisme *state-orchestrated partnership* yang memadukan peran pemerintah, industri, dan lembaga riset dalam satu ekosistem keamanan digital nasional (Israel National Cyber Directorate, 2021). Pendekatan ini memungkinkan integrasi fungsi intelijen, riset, dan industri dalam membangun ketahanan digital yang adaptif. Dalam *Applied Guide to Organizational Cyber Defense (ICDM v2)*, INCD menekankan pentingnya sinergi antara *incident response teams*, lembaga pendidikan, dan perusahaan teknologi dalam memperkuat kemampuan deteksi dini dan respons cepat terhadap ancaman digital (Israel National Cyber Directorate, 2023). Model kepemimpinan adaptif dan inovatif yang diterapkan Israel menjadi contoh bagaimana tata kelola keamanan siber dapat dioptimalkan melalui sinergi lintas aktor yang berorientasi pada inovasi teknologi pertahanan.

Berbeda dengan kedua negara tersebut, Rusia mengadopsi pendekatan yang lebih ofensif dan terpusat melalui strategi *information confrontation* yang termuat dalam *National Security Strategy of the Russian Federation*. Pendekatan ini mengintegrasikan operasi siber, perang informasi, serta aktivitas intelijen digital untuk mendukung tujuan geopolitik Rusia di kancah global (Government of the Russian Federation, 2021). Kajian strategis yang dilakukan oleh *Center for Strategic and International Studies (CSIS)* menunjukkan bahwa Rusia secara aktif menggunakan kekuatan sibernya untuk menyerang infrastruktur negara-negara Barat, mengintervensi opini publik, dan memperluas pengaruh geopolitiknya di ruang digital (CSIS, 2025). Pola kepemimpinan strategis-militer Rusia yang bersifat hierarkis menunjukkan bagaimana otoritas sentral dapat memperkuat efektivitas sistem pertahanan siber nasional, meskipun di sisi lain menimbulkan tantangan dalam hal transparansi dan akuntabilitas publik.

Ketimpangan kemampuan pertahanan siber antarnegara masih menunjukkan kesenjangan signifikan. Berdasarkan *Global Cybersecurity Index* (ITU, 2024), negara maju seperti Amerika Serikat dan Israel menempati peringkat tertinggi dalam hal kesiapan kebijakan, kapasitas kelembagaan, serta kualitas sumber daya manusia di bidang siber. Sebaliknya, negara berkembang, termasuk Indonesia, masih menghadapi berbagai keterbatasan dalam orkestrasi kebijakan nasional, pengembangan sumber daya manusia, dan infrastruktur digital pertahanan (Adma, 2023). Meskipun Indonesia telah membentuk Badan Siber dan Sandi Negara (BSSN) serta menetapkan *Strategi Keamanan Siber Nasional* sebagai langkah strategis menuju kemandirian digital (BSSN, 2024), masih terdapat tantangan berupa fragmentasi kelembagaan dan belum adanya doktrin pertahanan siber nasional yang komprehensif dan berkarakter Indonesia (BPK RI, 2023).

Melihat kompleksitas ancaman dan variasi model kepemimpinan global tersebut, penelitian ini bertujuan untuk menganalisis pola kepemimpinan Rusia, Amerika Serikat, dan Israel dalam pengelolaan sumber daya siber, serta menyusun pembelajaran strategis yang relevan bagi pembentukan doktrin pertahanan siber Indonesia. Penelitian ini

diharapkan dapat memberikan kontribusi konseptual dalam memperkuat integrasi antara dimensi kepemimpinan, strategi pertahanan, dan tata kelola teknologi, sehingga mampu meningkatkan ketahanan digital dan daya tangkal nasional terhadap ancaman siber masa depan (Susilo, 2025).

## METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan fokus pada analisis konseptual dan kebijakan (policy analysis) untuk memahami hubungan antara kepemimpinan strategis di domain siber pada tiga negara—Rusia, Amerika Serikat, dan Israel—dengan implikasinya terhadap pembentukan doktrin pertahanan siber Indonesia. Pendekatan ini dipilih karena memungkinkan peneliti menggali konteks, orientasi kebijakan, serta pola kepemimpinan secara mendalam, bukan sekadar mengukur hubungan kuantitatif antarvariabel (Adma, 2023). Melalui pendekatan ini, penelitian berupaya mengidentifikasi pola mobilisasi sumber daya siber, tata kelola digital, dan model kepemimpinan nasional yang diterapkan ketiga negara tersebut, kemudian merefleksikannya terhadap kebutuhan transformasi pertahanan siber Indonesia yang berlandaskan nilai Pancasila dan keamanan nasional (Susilo, 2025).

Sumber data penelitian ini berasal dari studi literatur dan dokumen resmi, baik nasional maupun internasional, yang memiliki relevansi dengan tema kepemimpinan strategis, keamanan siber, dan kebijakan pertahanan digital. Dokumen yang dianalisis meliputi kebijakan dan strategi nasional seperti *National Cybersecurity Strategy* dan *DoD Cyber Strategy* dari Amerika Serikat (The White House, 2023; U.S. Department of Defense, 2023); *Israel International Cyber Strategy* serta panduan *Industrialized Cyber Defense Methodology (ICDM v2)* dari Israel (Israel National Cyber Directorate, 2021, 2023); serta *National Security Strategy of the Russian Federation* yang menjadi dasar kebijakan siber Rusia (Government of the Russian Federation, 2021). Selain itu, penelitian ini juga menggunakan laporan dari lembaga kajian strategis seperti *Center for Strategic and International Studies (CSIS)* dan *Institut Montaigne*, yang membahas pendekatan Rusia terhadap *information confrontation* dan perang informasi (CSIS, 2025). Dari sisi nasional, sumber diperoleh dari *Strategi Keamanan Siber Nasional (BSSN)*, *Peraturan Presiden No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber*, serta artikel ilmiah nasional seperti *Jurnal Kajian Strategik Ketahanan Nasional* dan *Jurnal Pertahanan dan Bela Negara* (Adma, 2023; N. R. A. dkk., 2025; BSSN, 2024; Susilo, 2025).

Proses pengumpulan data dilakukan melalui telaah dokumen (documentary study), yaitu penelusuran sistematis terhadap bahan pustaka, dokumen kebijakan, laporan riset, dan publikasi ilmiah yang memiliki keterkaitan langsung dengan fokus penelitian. Penelusuran sumber dilakukan melalui basis data akademik seperti *Scopus*, *Taylor & Francis Online*, *JSTOR*, dan *Google Scholar*, serta portal resmi pemerintah dan lembaga pertahanan seperti *The White House*, *Israel National Cyber Directorate (INCD)*, *Ministry of Digital Development of the Russian Federation*, dan *Badan Siber dan Sandi Negara (BSSN)*. Tahapan telaah dilakukan secara berlapis mulai dari identifikasi sumber relevan,

ekstraksi informasi utama, hingga kategorisasi tematik berdasarkan dimensi kepemimpinan, kebijakan, dan strategi digital. Proses ini memastikan bahwa seluruh informasi yang digunakan bersifat kredibel, mutakhir, dan representatif untuk mendukung validitas temuan (ITU, 2024; BSSN, 2024).

Analisis data dilakukan dengan menggunakan metode analisis isi (content analysis) untuk mengidentifikasi tema-tema utama, pola konseptual, serta orientasi kebijakan yang berkaitan dengan kepemimpinan siber dan pertahanan digital. Analisis dilakukan secara deduktif, dimulai dari teori kepemimpinan transformasional (Bass & Riggio), adaptif (Heifetz), dan strategis-militer (Lykke) sebagai kerangka teoretis untuk menilai sejauh mana gaya kepemimpinan dan kebijakan siber ketiga negara tersebut dapat diadaptasi dalam konteks Indonesia (Israel National Cyber Directorate, 2023; Susilo, 2025). Proses analisis ini melibatkan beberapa tahapan utama, yaitu (1) reduksi data untuk menyeleksi informasi yang relevan; (2) kategorisasi konsep berdasarkan tema kepemimpinan, kebijakan, dan strategi pertahanan; serta (3) penarikan kesimpulan konseptual yang menggambarkan hubungan antara karakter kepemimpinan strategis dan efektivitas kebijakan siber (Adma, 2023; BPK RI, 2023; ITU, 2024).

Penelitian ini menitikberatkan kajian pada tiga aspek utama. Pertama, menelaah karakteristik kepemimpinan strategis Rusia, Amerika Serikat, dan Israel dalam merumuskan arsitektur pertahanan siber nasional, termasuk struktur kelembagaan dan model pengambilan keputusan strategis. Kedua, mengkaji mekanisme mobilisasi sumber daya digital dan kemitraan lintas-sektor—antara pemerintah, militer, industri, dan lembaga riset—yang menjadi landasan keberhasilan implementasi strategi keamanan siber di ketiga negara tersebut. Ketiga, menganalisis relevansi dan pembelajaran strategis dari ketiga model kepemimpinan tersebut bagi Indonesia dalam membangun doktrin pertahanan siber nasional yang adaptif, berkarakter nasional, dan selaras dengan nilai-nilai kejuangan TNI serta visi *Indonesia Emas 2045*. Ketiga aspek ini dianalisis secara triangulatif, dengan membandingkan teori, kebijakan, dan data empiris untuk menghasilkan pemahaman komprehensif, kontekstual, dan berbasis bukti ilmiah mengenai hubungan antara kepemimpinan strategis dan ketahanan siber nasional (Susilo, 2025).

Berkaitan dengan pendekatan tersebut, penelitian ini diharapkan dapat memberikan kontribusi akademis berupa penguatan teori kepemimpinan strategis dalam domain pertahanan siber, serta kontribusi praktis bagi pembuat kebijakan dalam merancang model kepemimpinan dan doktrin pertahanan siber Indonesia yang mampu mengintegrasikan teknologi, sumber daya manusia unggul, serta nilai-nilai Pancasila sebagai fondasi pertahanan digital nasional (Adma, 2023; N. R. A. dkk., 2025; Susilo, 2025).

## HASIL DAN PEMBAHASAN

Berdasarkan hasil kajian literatur terhadap berbagai sumber akademik, laporan kebijakan pertahanan, dan dokumen resmi dari Rusia, Amerika Serikat, Israel, serta Indonesia, diperoleh sejumlah temuan strategis yang relevan dengan fokus penelitian ini.

Kepemimpinan ketiga negara tersebut menunjukkan corak yang berbeda dalam mengelola sumber daya siber dan membangun ekosistem keamanan digital nasional. Amerika Serikat menampilkan kepemimpinan yang transformasional dan kolaboratif melalui sinergi lintas-lembaga dan sektor swasta; Rusia menonjol dengan kepemimpinan strategis-militer yang terpusat dan berorientasi ofensif; sedangkan Israel memperlihatkan kepemimpinan adaptif berbasis inovasi dan kemitraan lintas-sektor.

Analisis penelitian ini difokuskan pada tiga aspek utama. Pertama, menelaah karakteristik kepemimpinan strategis Rusia, Amerika Serikat, dan Israel dalam merumuskan arsitektur pertahanan siber nasional sebagai refleksi dari filosofi dan strategi keamanan masing-masing negara. Kedua, mengkaji mekanisme mobilisasi sumber daya digital serta pola kolaborasi lintas-sektor yang melibatkan pemerintah, militer, industri, dan lembaga riset dalam memperkuat ketahanan siber nasional. Ketiga, menganalisis relevansi dan pembelajaran strategis dari ketiga model kepemimpinan tersebut terhadap pembentukan doktrin pertahanan siber Indonesia yang berkarakter nasional, berlandaskan nilai-nilai Pancasila, serta berorientasi pada tujuan *Indonesia Emas 2045*.

Kepemimpinan strategis di domain siber mencerminkan orientasi politik, struktur kelembagaan, serta filosofi keamanan nasional masing-masing negara. Amerika Serikat menampilkan kepemimpinan transformasional dan kolaboratif, di mana visi keamanan digital diwujudkan melalui integrasi antara pemerintah, sektor swasta, akademisi, dan komunitas teknologi. Melalui *National Cybersecurity Strategy* dan *DoD Cyber Strategy*, pemerintah AS menegaskan prinsip *whole-of-nation approach* yang menempatkan ruang siber sebagai domain strategis sejajar dengan darat, laut, udara, dan antariksa (The White House, 2023; U.S. Department of Defense, 2023).

Berbeda dengan AS, Rusia menerapkan kepemimpinan strategis-militer yang hierarkis dan terpusat. Dokumen *National Security Strategy of the Russian Federation* menunjukkan orientasi geopolitik yang kuat melalui konsep *information confrontation*, yakni integrasi antara operasi siber, propaganda informasi, dan aktivitas intelijen digital untuk mendukung kebijakan luar negeri (Government of the Russian Federation, 2021). Model ini menggambarkan bahwa Rusia memandang ruang siber bukan hanya sebagai instrumen pertahanan, tetapi juga sebagai sarana ofensif untuk memperluas pengaruh global. Karakter kepemimpinan vertikal yang kuat menciptakan efisiensi komando dan kecepatan respons, meskipun di sisi lain menimbulkan keterbatasan transparansi dan partisipasi publik (CSIS, 2025).

Sementara itu, Israel mengembangkan kepemimpinan adaptif dan berbasis inovasi nasional. Melalui *Israel International Cyber Strategy* dan *Industrialized Cyber Defense Methodology (ICDM v2)*, Israel membangun struktur kelembagaan yang mengintegrasikan pemerintah, militer, industri, dan lembaga riset (Israel National Cyber Directorate, 2021, 2023). Pendekatan *state-orchestrated partnership* menjadikan negara sebagai fasilitator utama, sementara sektor swasta dan akademik menjadi motor penggerak inovasi teknologi pertahanan. Kekuatan utama model Israel terletak pada kemampuannya menyeimbangkan keamanan nasional dengan budaya inovasi terbuka, menjadikan sistem sibernya adaptif dan tangguh terhadap perubahan ancaman global.

Perbandingan karakter kepemimpinan siber antara Amerika Serikat, Rusia, dan Israel memperlihatkan variasi yang signifikan baik dalam orientasi strategi maupun pola tata kelola sumber daya digital. Tabel 1 berikut menggambarkan secara ringkas perbedaan fundamental di antara ketiganya, mencakup aspek karakter kepemimpinan, fokus strategi siber, serta ciri utama yang menjadi identitas masing-masing model.

**Tabel 1. Perbandingan Model Kepemimpinan Siber Tiga Negara**

Negara	Karakter Kepemimpinan	Fokus Strategi Siber	Ciri Utama
Amerika Serikat	Transformasional dan kolaboratif	Pertahanan proaktif dan kemitraan publik–swasta	Whole-of-nation approach, persistent engagement, koordinasi multi-lembaga
Rusia	Strategis-militer terpusat dan hierarkis	Dominasi informasi dan kontrol vertikal	Information confrontation, integrasi militer–intelijen, orientasi ofensif
Israel	Adaptif dan inovatif	Inovasi teknologi dan sinergi nasional	State–orchestrated partnership, ekosistem inovasi terbuka, integrasi sipil–militer

Ketiga negara menampilkan variasi dalam mekanisme mobilisasi sumber daya digital serta bentuk kolaborasi antaraktor strategis. Amerika Serikat mengembangkan model koordinasi multi-lembaga yang melibatkan *Department of Defense (DoD)*, *Cybersecurity and Infrastructure Security Agency (CISA)*, *Federal Bureau of Investigation (FBI)*, serta mitra industri teknologi. Sinergi ini memperkuat sistem deteksi dini, respons insiden, dan perlindungan infrastruktur kritis secara nasional (The White House, 2023). Kepemimpinan di tingkat strategis diperkuat oleh kerangka hukum dan kebijakan yang menempatkan keamanan digital sebagai tanggung jawab kolektif antara negara, industri, dan masyarakat.

Rusia, sebaliknya, mengedepankan pendekatan mobilisasi yang terpusat dan dikendalikan langsung oleh pemerintah melalui Kementerian Pertahanan, Dinas Keamanan Federal (FSB), dan lembaga intelijen siber. Mobilisasi sumber daya digital Rusia lebih bersifat militeristik, dengan dominasi negara atas aset teknologi strategis dan perusahaan digital nasional untuk mendukung keamanan siber (Government of the Russian Federation, 2021). Pendekatan ini memastikan koordinasi yang kuat dalam krisis, namun cenderung membatasi fleksibilitas inovasi lintas-sektor karena tingginya kontrol politik dan ketergantungan pada sumber daya negara (CSIS, 2025).

Sementara Israel menonjolkan kolaborasi lintas-sektor yang bersifat organik dan berkelanjutan. *Israel National Cyber Directorate (INCD)* berfungsi sebagai simpul utama antara pemerintah, industri, akademisi, dan komunitas profesional siber. Pendekatan ini

dikenal dengan konsep *ecosystem model*, di mana setiap aktor memainkan peran komplementer: pemerintah sebagai regulator dan pengarah kebijakan, industri sebagai inovator teknologi, serta lembaga riset sebagai penghasil pengetahuan strategis (Israel National Cyber Directorate, 2021). Hasilnya adalah sistem pertahanan siber yang efisien, berorientasi riset, serta adaptif terhadap dinamika ancaman global dan perkembangan teknologi mutakhir (Israel National Cyber Directorate, 2023).

Ketiga model kepemimpinan siber—Amerika Serikat, Rusia, dan Israel—memberikan pelajaran strategis yang berharga bagi Indonesia dalam membangun doktrin pertahanan siber nasional yang kokoh, berkarakter, dan berorientasi pada visi *Indonesia Emas 2045*. Doktrin ini tidak hanya berfungsi sebagai panduan operasional bagi TNI dan instansi pertahanan, tetapi juga sebagai pedoman nasional dalam menyinergikan kekuatan digital negara yang mencakup lembaga sipil, industri teknologi, akademisi, dan masyarakat siber.

Model Amerika Serikat menekankan kepemimpinan transformasional dan kolaboratif, di mana *National Cybersecurity Strategy* menampilkan prinsip *whole-of-nation approach* yang melibatkan pemerintah, sektor swasta, dan akademisi dalam satu visi keamanan digital nasional (The White House, 2023; U.S. Department of Defense, 2023). Bagi Indonesia, pendekatan ini relevan untuk memperkuat sinergi antara Kementerian Pertahanan, TNI, BSSN, serta sektor strategis lain agar kebijakan siber bersifat inklusif, kolaboratif, dan berkelanjutan (BSSN, 2024).

Dari Rusia, Indonesia dapat memetik pembelajaran tentang pentingnya kesiapan strategis dan ketegasan komando dalam menghadapi ancaman lintas batas. Konsep *information confrontation* menunjukkan perlunya sistem komando dan kontrol vertikal yang kuat untuk memastikan kecepatan respons terhadap serangan siber dan disinformasi (Government of the Russian Federation, 2021; CSIS, 2025). Namun, penerapan model ini perlu diadaptasi agar tetap berada dalam kerangka negara hukum dan prinsip demokrasi, sehingga keseimbangan antara keamanan nasional dan kebebasan digital dapat terjaga.

Adapun Israel memberikan inspirasi bagi penguatan kepemimpinan adaptif dan inovatif. Penerapan *Israel International Cyber Strategy* dan *ICDM v2* menunjukkan bahwa kemitraan strategis antara pemerintah, industri, dan lembaga riset mampu menciptakan ekosistem pertahanan siber yang kreatif, mandiri, dan berdaya saing global (Israel National Cyber Directorate, 2023). Bagi Indonesia, pendekatan ini menegaskan pentingnya membangun *triple helix collaboration* yang mempertemukan pemerintah, industri, dan akademisi dalam memperkuat inovasi teknologi, riset keamanan siber, serta kemandirian digital nasional.

Lebih jauh lagi, sintesis dari ketiga model kepemimpinan tersebut dapat menjadi fondasi konseptual bagi Indonesia dalam merumuskan doktrin pertahanan siber yang berkarakter nasional, kolaboratif, dan berorientasi inovasi. Doktrin ini perlu mengintegrasikan unsur transformasional (visioner dan inklusif seperti Amerika Serikat), strategis-militer (tegas dan responsif seperti Rusia), serta adaptif-inovatif (fleksibel dan berbasis riset seperti Israel). Kombinasi ini akan memperkuat arah kebijakan,



memperjelas struktur koordinasi kelembagaan, serta meningkatkan kapasitas inovasi nasional di bidang pertahanan digital.

Pembentukan doktrin pertahanan siber Indonesia harus berpijak pada nilai-nilai dasar nasional, di mana Pancasila menjadi landasan etis dan ideologis, nilai kejuangan TNI sebagai semangat pertahanan nonkonvensional, dan visi Indonesia Emas 2045 sebagai arah strategis menuju kemandirian dan kedaulatan digital (Susilo, 2025). Dalam tataran implementatif, penguatan arsitektur kelembagaan pertahanan siber lintas-matra perlu dilakukan melalui koordinasi antara TNI, BSSN, Kominfo, Polri, dan lembaga riset nasional. Selain itu, pengembangan SDM pertahanan digital harus menjadi prioritas melalui pendidikan militer berbasis teknologi, pelatihan keamanan siber terpadu, serta pembentukan pusat riset inovasi pertahanan nasional.

Dengan demikian, doktrin pertahanan siber Indonesia perlu bersifat proaktif, bukan reaktif, dalam menghadapi ancaman global. Doktrin ini berfungsi sebagai instrumen untuk memperkuat kedaulatan digital, meningkatkan daya tangkal nasional, serta memastikan transformasi pertahanan di era digital berjalan selaras dengan semangat Pancasila, prinsip demokrasi, dan visi Indonesia Emas 2045 (Susilo, 2025).

## KESIMPULAN

Berdasarkan hasil kajian dan analisis terhadap model kepemimpinan siber di tiga negara—Amerika Serikat, Rusia, dan Israel—dapat disimpulkan bahwa kepemimpinan strategis memiliki peran yang sangat fundamental dalam membentuk efektivitas sistem pertahanan digital suatu negara di era kompetisi multidomain. Ketiganya menunjukkan pendekatan yang berbeda dalam mengelola ruang siber sebagai domain strategis, namun memiliki kesamaan pandangan bahwa kekuatan nasional di abad ke-21 ditentukan oleh kemampuan memobilisasi sumber daya digital secara terintegrasi, berkelanjutan, dan berorientasi inovasi. Amerika Serikat menampilkan kepemimpinan transformasional dan kolaboratif melalui penerapan *whole-of-nation approach* yang mengutamakan sinergi antar-lembaga, sektor swasta, dan masyarakat digital. Rusia memperlihatkan kepemimpinan strategis-militer yang menekankan kontrol vertikal, efektivitas komando, dan konsistensi arah kebijakan dalam menjaga supremasi informasi nasional. Sementara itu, Israel menonjol dengan kepemimpinan adaptif-inovatif yang memadukan riset, teknologi, dan kemitraan lintas-sektor berbasis ekosistem. Sintesis dari ketiga model tersebut memberikan pelajaran penting bagi Indonesia dalam merumuskan doktrin pertahanan siber nasional yang berkarakter, kolaboratif, dan kontekstual. Doktrin ini perlu mengintegrasikan unsur transformasional untuk memperkuat koordinasi antarsektor, unsur strategis-militer untuk menjamin ketegasan dan kecepatan komando, serta unsur adaptif-inovatif untuk membangun kemandirian riset dan teknologi siber nasional. Dengan mengharmonisasikan ketiga dimensi tersebut, Indonesia dapat mengembangkan model kepemimpinan strategis di bidang pertahanan siber yang berlandaskan nilai-nilai Pancasila, berorientasi pada kedaulatan digital, serta mendukung pencapaian visi *Indonesia Emas 2045* secara berkelanjutan.

## BIBLIOGRAFI

- Adma, A. (2023). *Transformasi sistem pertahanan siber Indonesia dengan pendekatan sistemik-holistik*. Jurnal Kajian Strategik Ketahanan Nasional, 6(1).
- Badan Pemeriksa Keuangan Republik Indonesia (BPK RI). (2023). *Peraturan Presiden No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber*. Jakarta.
- Badan Siber dan Sandi Negara (BSSN). (2024). *Strategi Keamanan Siber Nasional Republik Indonesia*. Jakarta.
- Center for Strategic and International Studies (CSIS). (2025). *Russia's Shadow War Against the West*. Washington, D.C.
- Government of the Russian Federation. (2021). *National Security Strategy of the Russian Federation*. Moscow.
- Israel National Cyber Directorate. (2021). *Israel International Cyber Strategy*. Tel Aviv.
- Israel National Cyber Directorate. (2023). *Applied Guide to Organizational Cyber Defense (ICDM v2)*. Tel Aviv.
- International Telecommunication Union (ITU). (2024). *Global Cybersecurity Index*. Geneva.
- N. R. A., M., et al. (2025). *Kesenjangan Kapabilitas Keamanan Siber Indonesia 2020–2025*. Triwikrama: Jurnal Kebijakan Publik.
- Susilo, T. (2025). *Kepemimpinan digital dan urgensi doktrin pertahanan siber nasional*. Jurnal Pertahanan dan Bela Negara, 14(2).
- The White House. (2023). *National Cybersecurity Strategy*. Washington, D.C.
- U.S. Department of Defense. (2023). *DoD Cyber Strategy – Unclassified Summary*. Washington, D.C.
- 

**First publication right:**

[Jurnal Syntax Fusion: Jurnal Nasional Indonesia](#)

**This article is licensed under:**

