

**TRANSFORMASI KEPEMIMPINAN DIGITAL DALAM DOKTRIN PERTAHANAN: STUDI PERBANDINGAN RUSIA, AMERIKA SERIKAT, DAN ISRAEL SEBAGAI BASIS PENGUATAN PERTAHANAN SIBER INDONESIA**

**Petrus Bambang Setya Budi**

Sekolah Staf dan Komando Tentara Nasional Indonesia

[petrusbsb@gmail.com](mailto:petrusbsb@gmail.com)

**Gatot Dwi Nugroho**

Sekolah Staf dan Komando Tentara Nasional Indonesia

[masgatot172@gmail.com](mailto:masgatot172@gmail.com)

**Tarsisius Susilo**

Sekolah Staf dan Komando Tentara Nasional Indonesia

[muchus70@gmail.com](mailto:muchus70@gmail.com)

**Gusti Bagus Oka Tapayasa**

Sekolah Staf dan Komando Tentara Nasional Indonesia

**H.D. Arifin Simanjuntak**

Sekolah Staf dan Komando Tentara Nasional Indonesia

**Abstract**

*This study examines the transformation of digital leadership in defense doctrines, focusing on lessons from Russia, the United States, and Israel, and their implications for the urgency of establishing an Indonesian cyber defense doctrine. The research employs a literature-based approach through strategic comparative studies, policy analysis, and global benchmarking. Findings reveal that Russia emphasizes digital sovereignty through strategic information control; the United States prioritizes multisectoral collaboration and technological innovation; while Israel highlights leadership flexibility and the development of digital human capital. Benchmarking indicates that Indonesia should integrate these three approaches in formulating a national cyber defense doctrine rooted in Pancasila values, national interests, and the principle of state sovereignty. Therefore, the establishment of a cyber defense doctrine in Indonesia is a strategic necessity to strengthen national security, protect critical infrastructure, and develop adaptive digital leadership in the era of technological disruption.*

**Keywords:** digital leadership, defense doctrine, cyber security, Russia, United States, Israel, Indonesia

**Abstrak**

Penelitian ini membahas transformasi kepemimpinan digital dalam doktrin pertahanan dengan fokus pada pembelajaran dari Rusia, Amerika Serikat, dan Israel, serta implikasinya bagi urgensi pembentukan doktrin pertahanan siber Indonesia. Penelitian menggunakan metode studi literatur dengan pendekatan studi perbandingan strategis, analisis kebijakan, serta benchmarking global. Hasil penelitian menunjukkan bahwa Rusia menekankan kedaulatan digital melalui kontrol informasi strategis; Amerika Serikat mengedepankan kolaborasi multisektor dan inovasi teknologi; sedangkan Israel menonjol melalui fleksibilitas kepemimpinan dan penguatan sumber daya manusia digital. Benchmarking memperlihatkan bahwa Indonesia perlu mengintegrasikan ketiga pendekatan tersebut dalam merumuskan doktrin pertahanan siber nasional yang berbasis nilai Pancasila, kepentingan

nasional, dan prinsip kedaulatan negara. Dengan demikian, pembentukan doktrin pertahanan siber di Indonesia menjadi sebuah urgensi strategis untuk memperkuat keamanan nasional, melindungi infrastruktur vital, serta mewujudkan kepemimpinan digital yang adaptif di era disruptif teknologi.

**Kata kunci:** kepemimpinan digital, doktrin pertahanan, keamanan siber, Rusia, Amerika Serikat, Israel, Indonesia

## PENDAHULUAN

Perkembangan teknologi digital telah menciptakan lanskap keamanan internasional yang sepenuhnya baru. Ancaman siber kini tidak hanya terbatas pada pencurian data atau peretasan sistem, melainkan juga menyerang infrastruktur kritis seperti jaringan listrik, sistem perbankan, dan bahkan pertahanan militer. Menurut laporan *Global Cybersecurity Index* yang diterbitkan International Telecommunication Union (ITU, 2021), lebih dari 80% negara di dunia telah mengintegrasikan keamanan siber dalam strategi pertahanan nasional mereka. Hal ini menunjukkan bahwa ruang siber telah menjadi domain strategis yang sama pentingnya dengan darat, laut, udara, dan luar angkasa.

Dalam konteks ini, kepemimpinan digital memainkan peran sentral. Kepemimpinan digital tidak hanya berarti kemampuan menggunakan teknologi, tetapi juga kapasitas strategis untuk memobilisasi sumber daya digital, mengintegrasikan kebijakan, dan memastikan keamanan nasional dalam ruang siber. Rusia, Amerika Serikat, dan Israel merupakan contoh negara yang berhasil membangun kepemimpinan digital di bidang pertahanan dengan cara yang berbeda. Ketiganya menunjukkan bagaimana transformasi kepemimpinan digital dapat memengaruhi efektivitas doktrin pertahanan siber.

Perkembangan teknologi informasi dan komunikasi (TIK) telah membawa transformasi besar dalam lanskap keamanan global. Jika pada abad ke-20 pertahanan negara didominasi oleh kekuatan konvensional di darat, laut, dan udara, maka pada abad ke-21 domain baru muncul: **siber** dan **informasi**. Serangan tidak lagi hanya berbentuk fisik, tetapi juga digital melalui peretasan infrastruktur kritikal, pencurian data strategis, sabotase perangkat lunak, hingga disinformasi yang mampu menggoyahkan stabilitas sosial-politik sebuah negara. Dengan demikian, kepemimpinan dalam pertahanan modern tidak bisa dilepaskan dari kemampuan mengelola sumber daya digital, informasi, dan teknologi secara strategis.

Sejumlah negara telah membuktikan bagaimana kepemimpinan berperan penting dalam membentuk arah kebijakan pertahanan siber. Amerika Serikat, misalnya, menekankan kolaborasi publik-swasta dalam melindungi infrastruktur kritikal serta menerapkan strategi *Defend Forward* untuk mencegah ancaman siber sebelum mencapai wilayah domestik. Israel menonjol melalui kepemimpinan adaptif yang berfokus pada inovasi, integrasi talenta, dan ekosistem startup, sehingga menjadi salah satu negara dengan kesiapan siber paling tinggi di dunia. Sementara itu, Rusia memilih pendekatan yang menekankan pada kontrol ruang informasi domestik, kedaulatan digital, dan penggunaan operasi informasi sebagai instrumen geopolitik. Ketiga model ini menunjukkan keragaman gaya kepemimpinan dalam mengelola ruang siber sekaligus memperlihatkan bahwa tidak ada satu formula tunggal yang berlaku universal.

Bagi Indonesia, urgensi pengembangan doktrin pertahanan siber nasional menjadi semakin jelas. Keberadaan Badan Siber dan Sandi Negara (BSSN), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta strategi keamanan siber yang sedang digodok

menunjukkan adanya kemajuan signifikan. Namun demikian, kerangka pertahanan siber Indonesia saat ini masih lebih banyak bersifat normatif dan kelembagaan, belum sepenuhnya operasional dalam bentuk doktrin pertahanan terpadu yang dapat menjadi pedoman komprehensif bagi TNI, kementerian/lembaga, sektor swasta, hingga masyarakat. Tantangan yang dihadapi Indonesia semakin kompleks, mulai dari serangan ransomware terhadap institusi pemerintah, kebocoran data publik, hingga perang informasi yang berpotensi memengaruhi kohesi nasional.

Indonesia sendiri menghadapi tantangan yang semakin kompleks. Laporan BSSN (2023) mencatat lebih dari 200 juta serangan siber yang menargetkan sektor pemerintahan, keuangan, dan infrastruktur kritis sepanjang tahun. Ancaman ini menunjukkan bahwa tanpa doktrin pertahanan siber yang jelas dan kuat, kedaulatan digital Indonesia akan berada dalam posisi rentan. Oleh karena itu, penelitian ini menekankan pentingnya merumuskan doktrin pertahanan siber Indonesia yang berbasis nilai, berorientasi pada keamanan nasional, serta didukung oleh kepemimpinan digital yang adaptif.

Laporan **ASEAN Cybersecurity Cooperation Strategy (2021–2025)** dan **Global Cybersecurity Index (ITU, 2021)** menempatkan Indonesia di peringkat menengah dalam kesiapan siber regional. Hal ini menunjukkan bahwa meskipun ada kemajuan signifikan melalui pembentukan BSSN dan peningkatan koordinasi lintas lembaga, Indonesia masih menghadapi kesenjangan dalam aspek regulasi, literasi siber, serta kesiapan sumber daya manusia. Dengan kata lain, penyusunan doktrin pertahanan siber yang berbasis pada *cyber deterrence* tidak hanya diperlukan untuk menghadapi ancaman eksternal, tetapi juga untuk memperkuat posisi tawar Indonesia dalam diplomasi siber di kawasan ASEAN dan Indo-Pasifik.

Selain itu, faktor nilai dan jati diri bangsa menjadi elemen penting. Doktrin pertahanan siber Indonesia tidak hanya harus mampu menghadapi ancaman teknis, tetapi juga perlu selaras dengan **nilai Pancasila, UUD 1945, dan prinsip keamanan nasional**. Dengan demikian, doktrin ini tidak hanya berbasis pada *best practices* internasional, tetapi juga berakar pada kepentingan strategis nasional yang menekankan kedaulatan digital, perlindungan hak warga, dan pertahanan maritim yang kuat mengingat posisi geostrategis Indonesia sebagai negara kepulauan terbesar di dunia.

Dalam konteks geopolitik kawasan, urgensi doktrin pertahanan siber Indonesia semakin nyata ketika dikaitkan dengan dinamika Indo-Pasifik. Kawasan ini saat ini menjadi salah satu arena kompetisi strategis terbesar di dunia, terutama antara Amerika Serikat dan Tiongkok. Rivalitas kedua negara bukan hanya berlangsung di ranah militer konvensional, tetapi juga di ranah digital dan siber. Tiongkok, misalnya, melalui inisiatif *Digital Silk Road* sebagai bagian dari *Belt and Road Initiative (BRI)*, berupaya memperluas pengaruhnya di bidang infrastruktur digital dengan membangun jaringan telekomunikasi, satelit, hingga teknologi 5G. Bagi Indonesia, keterlibatan dalam proyek-proyek digital semacam ini membuka peluang akelerasi transformasi teknologi, tetapi sekaligus menghadirkan kerentanan baru terkait ketergantungan pada infrastruktur asing dan risiko penyalahgunaan data strategis.

Selain itu, kawasan Indo-Pasifik dikenal rawan konflik, salah satunya di **Laut Cina Selatan**. Perselisihan klaim teritorial tidak hanya berdampak pada aspek pertahanan maritim, tetapi juga pada aspek digital. Serangan siber kerap digunakan sebagai instrumen *hybrid warfare* untuk menekan lawan tanpa konfrontasi langsung. Beberapa laporan intelijen mencatat peningkatan aktivitas peretasan yang diduga berasal dari aktor-aktor negara di kawasan, yang menargetkan kementerian,

lembaga riset, dan infrastruktur energi negara-negara ASEAN. Indonesia, sebagai negara dengan posisi strategis di kawasan ini, berpotensi besar menjadi target baik sebagai pihak yang bersengketa maupun sebagai negara penghubung jalur perdagangan digital dan maritim.

Lebih jauh, laporan *Cybersecurity Ventures* (2022) memperkirakan kerugian ekonomi global akibat kejahatan siber akan mencapai USD 10,5 triliun pada tahun 2025. Angka ini menempatkan kejahatan siber sebagai salah satu ancaman ekonomi terbesar, bahkan melampaui perdagangan narkotika ilegal. Indonesia sendiri, dengan lebih dari 210 juta pengguna internet dan tingkat adopsi digital yang sangat cepat, menghadapi risiko kebocoran data, serangan *ransomware*, dan sabotase infrastruktur vital yang dapat melumpuhkan layanan publik maupun sektor ekonomi. Hal ini diperkuat oleh fakta bahwa transformasi digital Indonesia masih sering tidak diimbangi dengan perlindungan keamanan siber yang memadai.

Konsekuensi lain dari perkembangan ini adalah munculnya kebutuhan akan kepemimpinan digital yang mampu mengantisipasi ancaman lintas batas. Kepemimpinan yang dimaksud tidak hanya terbatas pada pemimpin politik, tetapi juga mencakup pemimpin institusi, lembaga keamanan, dan sektor swasta yang mengelola data serta infrastruktur digital kritis. Dalam kerangka ini, Indonesia membutuhkan doktrin pertahanan siber yang berfungsi sebagai panduan strategis dalam menghadapi tantangan global maupun regional, dengan merujuk pada praktik terbaik negara-negara seperti Rusia, Amerika Serikat, dan Israel. Doktrin tersebut tidak boleh hanya bersifat reaktif, tetapi harus proaktif, berbasis nilai nasional, dan terintegrasi dengan dinamika geopolitik Indo-Pasifik.

Selain dinamika geopolitik dan perkembangan teknologi, isu *cyber deterrence* juga menjadi faktor penting yang menegaskan urgensi pembentukan doktrin pertahanan siber Indonesia. Konsep ini menekankan kemampuan suatu negara untuk mencegah serangan dengan menunjukkan kesiapan, kekuatan, dan kapasitas responsif yang dapat menimbulkan konsekuensi serius bagi penyerang. Rusia, Amerika Serikat, dan Israel telah menunjukkan variasi pendekatan *deterrence by punishment* maupun *deterrence by denial* melalui pembangunan infrastruktur pertahanan siber yang tangguh. Indonesia, yang saat ini masih berada pada tahap penguatan kapasitas dasar, membutuhkan doktrin pertahanan siber yang terstruktur agar mampu membangun kepercayaan nasional dan internasional mengenai kemampuan pertahanannya.

Dengan demikian, urgensi penyusunan doktrin pertahanan siber bagi Indonesia tidak dapat dilepaskan dari konteks keamanan kawasan Indo-Pasifik. Posisi strategis Indonesia di tengah rivalitas kekuatan besar dunia menjadikannya rentan sekaligus memiliki peluang untuk mengambil peran sebagai pemimpin regional dalam keamanan siber. Untuk itu, pembelajaran dari negara-negara dengan kepemimpinan digital yang kuat sangat relevan, sekaligus harus diadaptasi dengan identitas dan kepentingan nasional Indonesia. Berdasarkan latar belakang tersebut, tulisan ini bertujuan untuk:

1. Mengkaji perbandingan gaya kepemimpinan dalam mengelola sumber daya siber dan informasi di Rusia, Amerika Serikat, dan Israel.
2. Mengidentifikasi pelajaran penting yang relevan bagi Indonesia dalam membangun kepemimpinan era digital di bidang pertahanan.
3. Merumuskan kerangka awal doktrin pertahanan siber Indonesia yang berbasis nilai, berorientasi pada keamanan nasional, serta adaptif terhadap dinamika ancaman global.

## Tinjauan Pustaka

### 1. Konsep Siber dan Pertahanan

Domain siber didefinisikan sebagai ruang operasi yang melibatkan jaringan komputer, sistem informasi, perangkat keras, perangkat lunak, serta interaksi manusia di dalamnya. Menurut Nye (2010), kekuatan siber (*cyber power*) adalah kemampuan suatu aktor untuk memperoleh tujuan melalui penggunaan sumber daya di ruang siber. Dalam konteks pertahanan, ruang siber bukan hanya soal teknologi, tetapi juga dimensi informasi yang mencakup arus data, narasi, dan persepsi publik. Oleh karena itu, sejumlah negara menyatukan konsep **cybersecurity** dengan **information warfare** (perang informasi).

### 2. Kepemimpinan Era Digital dan Siber

Kepemimpinan era digital menuntut adaptasi dari model konvensional menuju model yang berbasis visi, orkestrasi lintas aktor, serta pengelolaan talenta digital. Northouse (2022) menyebutkan tiga dimensi utama kepemimpinan modern:

- Visioning** – kemampuan merumuskan arah strategis dalam menghadapi ketidakpastian;
- Orchestration** – keterampilan mengintegrasikan berbagai pemangku kepentingan, baik sipil maupun militer;
- Adaptive Capability** – membangun organisasi pembelajar (*learning organization*) yang tanggap terhadap ancaman baru.

Dalam konteks pertahanan siber, kepemimpinan bukan hanya teknis, tetapi juga politik dan strategis, yakni bagaimana pemimpin membangun legitimasi, mengalokasikan sumber daya, serta membentuk doktrin yang bisa dioperasionalkan.

### 3. Kepemimpinan Amerika Serikat

Model kepemimpinan kolaboratif (networked leadership) mengandalkan kerja sama sipil, militer, dan swasta. Kepemimpinan pertahanan siber Amerika Serikat ditandai dengan integrasi antara militer, lembaga sipil, dan sektor swasta. Menurut Healey (2019) dalam Journal of Cyber Policy, strategi persistent engagement dan defend forward menjadi dasar pendekatan AS. Strategi ini menekankan pencegahan proaktif, yakni melakukan operasi siber di luar jaringan domestic untuk mencegah serangan sebelum mencapai infrastruktur nasional. Selain itu, laporan dari U.S Departement of Defense (2023) menunjukkan bahwa keberhasilan strategi ini sangat bergantung pada kepemimpinan yang kolaboratif. Komandan USCYBERCOM berperan memberikan arah strategis, sementara Lembaga seperti Cybersecurity and Infrastructure Security Agency (CISA) bertugas mengamankan sektor sipil, dan perusahaan swasta diwajibkan menerapkan standart keamanan minimum. Hal ini menverminkan model networked leadership-pemimpin membangun kerangka kerja sama lintas sektor untuk melindungi ekosistem digital secara menyeluruh.

### 4. Kepemimpinan Israel

Model kepemimpinan inovatif (mission-driven leadership) menekankan adaptasi, talenta, dan inovasi. Israel menampilkan gaya kepemimpinan siber yang adaptif dan berorientasi pada inovasi. Menurut Siboni & Siman-Tov (2014) dalam Military and Strategic Affairs Journal, Israel berhasil membangun Israel National Cyber Directorate (INCD) sebagai pusat komando sipil yang mengatur pertahanan siber nasional. INCD berfungsi sebagai single point of accountability, mengintegrasikan sektor militer, intelejen, akademik, dan swasta. Lebih lanjut, penelitian oleh Tabansky & Ben-Israel

(2015) di Cybersecurity Review menegaskan bahwa keunggulan Israel terletak pada “triple helix” kepemimpinan: negara, industri, dan akademisi. Model ini memungkinkan kepemimpinan sipil untuk mengambil keputusan cepat, sambil memanfaatkan talenta digital melalui program pendidikan, startup teknologi, serta proyek pertahanan. Kepemimpinan digital di Israel bersifat mission-driven, dengan fokus pada keberlangsungan inovasi dan respons adaptif terhadap serangan.

#### 5. Kepemimpinan Rusia

Model kepemimpinan terpusat (centralized leadership) fokus pada kedaulatan digital dan kontrol informasi domestik. Rusia mengadopsi pendekatan berbeda yang menekankan pada konsep keamanan informasi (*information security*). Doktrin keamanan informasi Rusia (2016) menegaskan bahwa ancaman terhadap ruang informasi domestik sama seriusnya dengan ancaman militer. Menurut Connell & Vogler (2017) dalam laporan *Army Cyber Institute*, kepemimpinan Rusia beruaya mengintegrasikan operasi teknis (serangan dan pertahanan siber) dengan operasi psikologis seperti propaganda dan disinformasi. Negara mengontrol infrastruktur internet domestik (dikenal sebagai konsep “RuNet”) serta memperkuat kedaulatan digital dengan membatasi akses dan arus informasi asing. Hal ini memperlihatkan bahwa kepemimpinan Rusia mengutamakan stabilitas internal melalui kontrol informasi, berbeda dengan AS yang menekankan kerja sama terbuka atau Israel yang menekankan inovasi.

#### 6. Pertahanan Siber Indonesia

Indonesia telah mengambil langkah dengan membentuk Badan Siber dan Sandi Negara (BSSN) serta menerbitkan Undang-Undang Nomor 27 Tahun 2022 tentang perlindungan Data Pribadi. Namun, sejumlah penelitian (Pratama, 2022; BSSN, 2023) menyoroti bahwa kerangka pertahanan Indonesia masih bersifat fragmentaris. Belum ada doktrin pertahanan siber nasional yang menyatukan aktor militer, sipil, dan swasta dalam satu kerangka operasional. Selain itu, literatur juga menggaribawahi pentingnya dimensi nilai dan ideologi nasional. Menurut Santoso (2021), pembentukan doktrin pertahanan Indonesia harus berakar pada Pancasila, UUD 1945, serta kepentingan nasional agar tidak sekadar mengadopsi model negara lain, melainkan menyesuaikan dengan konteks sosial, politik, dan geostategis Indonesia sebagai negara kepulauan dan demokrasi terbesar di Asia Tenggara. Tantangan untuk Indonesia yaitu ketergantungan pada teknologi asing, dimana Indonesia masih sangat bergantung pada teknologi asing, baik dari sisi perangkat keras (server, jaringan, satelit) maupun perangkat lunak (sistem operasi, aplikasi keamanan, AI). Hal ini menimbulkan kerentanan kedaulatan digital, karena pihak asing berpotensi mengendalikan, menyusup, atau memanfaatkan infrastuktur strategi Indonesia. Kurangnya SDM unggul, berdasarkan laporan BSSN (2022) menyebutkan bahwa kebutuhan tenaga ahli keamanan siber mencapai ratusan ribu, sementara yang tersedia baru sebagian kecil. Israel sukses membangun unit elit siber (Unit 8200) dengan basis pelatihan sejak muda. Amerika Serikat bekerja sama dengan universitas untuk mencetak *cyber warriors* tanpa doktrin pertahanan sier yang memprioritaskan pengembangan SDM unggul, Indonesia beresiko hanya menjadi konsumen teknologi, bukan pelaku strategis. Lemahnya integritas antarinstansi adalah tantangan yang terakhir bagi Indonesia.

#### 7. Kerangka Teoritis

Kajian tentang pertahanan siber membutuhkan pijakan teoritis yang komprehensif agar analisis tidak hanya deskriptif, tetapi juga memiliki basis konseptual dalam tradisi ilmu hubungan internasional, studi keamanan, dan kepemimpinan. Dengan demikian, doktrin pertahanan siber

Indonesia dapat dipahami sebagai hasil dialektika antara kekuatan material, kerja sama institusional, serta konstruksi nilai dan identitas bangsa.

Dalam paradigma realisme klasik, sebagaimana dipaparkan oleh Hans Morgenthau (1948), negara adalah aktor utama yang mengejar kepentingan nasional melalui kekuatan. Dalam konteks dunia digital, ruang siber diperlakukan sebagai *domain baru* yang setara dengan darat, laut, udara, dan luar angkasa. Rusia merepresentasikan logika ini melalui strategi *state-centric* yang menempatkan pemerintah sebagai pengendali penuh informasi digital, sekaligus memanfaatkan serangan siber ofensif untuk memperluas pengaruh geopolitik.

Neorealisme Kenneth Waltz (1979) lebih lanjut menekankan struktur internasional yang anarkis. Persaingan di ruang siber mencerminkan kondisi ini, karena tidak ada otoritas tunggal yang mengatur perilaku negara secara mutlak. Setiap negara berusaha memperkuat kapabilitas sibernya agar tidak tertinggal. Dalam kerangka ini, pertahanan siber Indonesia perlu dilihat sebagai upaya menjaga *survival* negara dalam sistem internasional yang kompetitif.

Liberalisme menyoroti pentingnya kerja sama, aturan, dan institusi internasional. Joseph Nye (2004) memperkenalkan konsep *soft power*, yang juga relevan dalam konteks siber: pengaruh dapat dibangun melalui norma, nilai, dan inovasi digital. Amerika Serikat mengadopsi pendekatan ini dengan mendorong kemitraan antara negara, sektor swasta, dan organisasi internasional.

Neoliberalisme institusional menegaskan bahwa institusi internasional mampu menurunkan biaya transaksi dan membangun kepercayaan antarnegara. Contohnya adalah NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) yang menjadi forum pertukaran pengetahuan dan strategi pertahanan siber. Bagi Indonesia, kerja sama di ASEAN melalui ASEAN Cybersecurity Cooperation Strategy merupakan cerminan logika neoliberalisme dalam menghadapi ancaman lintas batas.

Konstruktivisme, sebagaimana dipaparkan oleh Alexander Wendt (1992), menekankan bahwa *anarchy is what states make of it*. Artinya, ruang siber bukan sekadar arena teknis, tetapi juga sarat makna sosial, nilai, dan identitas. Israel merupakan contoh nyata: identitas sebagai bangsa yang dikelilingi ancaman melahirkan strategi pertahanan siber berbasis mobilisasi nasional dan inovasi teknologi. Bagi Indonesia, konstruktivisme menegaskan bahwa doktrin pertahanan siber tidak boleh sekadar meniru negara lain, melainkan harus dikonstruksi berdasarkan nilai Pancasila, kepentingan nasional, serta prinsip kedaulatan digital.

Copenhagen School melalui Barry Buzan, Ole Wæver, dan Jaap de Wilde (1998) memperkenalkan teori sekuritisasi, yaitu proses ketika suatu isu dianggap sebagai ancaman eksistensial sehingga memerlukan tindakan luar biasa (*extraordinary measures*). Dalam konteks siber, serangan terhadap infrastruktur kritis seperti energi, transportasi, dan perbankan dapat dikategorikan sebagai ancaman eksistensial yang mengancam keberlangsungan negara.

Bagi Indonesia, proses sekuritisasi ini penting untuk mendorong pembentukan doktrin pertahanan siber. Dengan menyatakan ancaman siber sebagai isu keamanan nasional, pemerintah dapat memperoleh legitimasi politik untuk membangun institusi, regulasi, dan alokasi anggaran yang lebih besar.

Selain teori hubungan internasional, kerangka analisis juga membutuhkan teori kepemimpinan digital. Menurut Avolio & Kahai (2003), kepemimpinan digital mencakup kemampuan pemimpin dalam mengintegrasikan teknologi informasi dengan visi strategis organisasi. Teori *transformational*

*leadership* (Bass, 1990) menekankan pentingnya inspirasi, motivasi, dan inovasi dalam membawa perubahan. Hal ini tercermin dalam kepemimpinan AS yang mampu menggerakkan sektor swasta dalam menghadapi ancaman siber. Sementara itu, teori *adaptive leadership* (Heifetz, 1994) menyoroti pentingnya fleksibilitas dalam menghadapi ketidakpastian. Israel menampilkan praktik kepemimpinan adaptif dengan melibatkan masyarakat sipil, akademisi, dan militer dalam strategi sibernya. Indonesia dapat belajar dari model ini untuk menciptakan kepemimpinan digital yang kolaboratif dan kontekstual.

Dengan menggabungkan realisme, liberalisme, konstruktivisme, teori sekuritisasi, dan teori kepemimpinan digital, maka doktrin pertahanan siber Indonesia perlu dirancang dengan pendekatan multidimensional:

- a. Realisme → menjaga kedaulatan digital dan kekuatan negara.
- b. Liberalisme → memperkuat kerja sama regional dan global.
- c. Konstruktivisme → menanamkan nilai Pancasila, identitas nasional, dan norma etika digital.
- d. Sekuritisasi → memastikan isu siber diprioritaskan dalam kebijakan nasional.
- e. Kepemimpinan digital → membangun visi strategis yang adaptif, kolaboratif, dan inovatif.

Dengan fondasi ini, Indonesia dapat mengembangkan doktrin pertahanan siber yang tidak hanya reaktif terhadap ancaman, tetapi juga proaktif dalam menciptakan ekosistem digital yang aman, inklusif, dan berdaya saing global.

## METODE PENELITIAN

### 1. Jenis dan Pendekatan Penelitian

Penelitian ini merupakan penelitian kualitatif dengan metode studi perbandingan strategis (*comparative strategic studies*) dan analisis kebijakan (*policy analysis*). Studi perbandingan strategis digunakan untuk menganalisis pola kepemimpinan digital dan doktrin pertahanan siber di Rusia, Amerika Serikat, dan Israel, dengan tujuan menemukan persamaan, perbedaan, dan relevansi strategis bagi Indonesia. Analisis kebijakan digunakan untuk mengkaji bagaimana pelajaran dari ketiga negara dapat menjadi dasar dalam perumusan doktrin pertahanan siber Indonesia yang berbasis nilai nasional dan keamanan negara.

Penelitian ini menggunakan data sekunder yang diperoleh melalui penelusuran berbagai literatur yang relevan dengan tema kepemimpinan digital dan doktrin pertahanan siber. Data sekunder dipilih karena penelitian berfokus pada analisis konseptual dan perbandingan strategis antarnegara, bukan pada pengumpulan data primer di lapangan. Oleh karena itu, sumber data yang digunakan mencakup dokumen resmi, publikasi akademik, laporan lembaga riset, serta sumber kontekstual yang kredibel.

### 2. Sumber Data

Pertama, dokumen resmi pertahanan menjadi rujukan utama untuk memahami secara langsung arah kebijakan dan doktrin siber tiap negara. Misalnya, *National Cyber Strategy* yang diterbitkan oleh Departemen Pertahanan Amerika Serikat (DoD) digunakan untuk melihat bagaimana kepemimpinan digital dan strategi siber AS dibangun melalui inovasi teknologi dan kerja sama internasional. Sementara itu, *Military Doctrine of the Russian Federation* memberikan gambaran mengenai orientasi Rusia yang menekankan perang informasi dan kontrol negara atas ruang digital. Adapun laporan keamanan siber yang diterbitkan oleh Israel Defense Forces (IDF) menjadi acuan

dalam menelaah fleksibilitas kepemimpinan digital Israel serta pengembangan unit siber elit seperti Unit 8200.

Kedua, literatur akademik berupa artikel jurnal, buku, prosiding, serta disertasi digunakan untuk memperkaya analisis teoretis. Literatur ini memberikan landasan konseptual mengenai hubungan antara kepemimpinan digital, keamanan siber, dan doktrin pertahanan. Artikel yang diterbitkan dalam jurnal internasional seperti *Journal of Strategic Studies*, *Cyber Defense Review*, atau publikasi dari universitas terkemuka menjadi rujukan dalam membangun kerangka analisis.

Ketiga, laporan kebijakan dan publikasi think-tank internasional digunakan untuk memberikan perspektif analitis terhadap dinamika keamanan siber global. Lembaga seperti RAND Corporation, Chatham House, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), serta lembaga nasional seperti Badan Siber dan Sandi Negara (BSSN) dan Kementerian Pertahanan RI menjadi referensi penting. Laporan-laporan tersebut menyoroti isu-isu aktual seperti ancaman terhadap infrastruktur kritis, strategi pertahanan digital, serta urgensi kedaulatan siber nasional.

Keempat, penelitian ini juga menggunakan sumber kontekstual berupa analisis media internasional dan laporan organisasi multilateral. Sumber ini berfungsi untuk memberikan data empiris mengenai kasus serangan siber global dan regional, seperti serangan Rusia dalam konflik Ukraina, gangguan infrastruktur energi di Amerika Serikat akibat malware, serta operasi intelijen siber Israel. Data kontekstual ini membantu memperjelas bagaimana doktrin dan kepemimpinan digital diterapkan dalam praktik nyata.

Dengan memadukan berbagai jenis sumber data tersebut, penelitian ini memperoleh gambaran yang komprehensif, kredibel, dan triangulatif. Data yang bersumber dari dokumen resmi memberikan dasar normatif, literatur akademik memperkuat aspek teoretis, laporan think-tank menambah perspektif strategis, sedangkan data kontekstual menghadirkan ilustrasi empiris. Keempatnya saling melengkapi untuk mendukung analisis perbandingan strategis dan formulasi kebijakan doktrin pertahanan siber Indonesia.

### 3. Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan melalui penelusuran literatur yang bersifat sistematis dan terarah. Karena penelitian ini menggunakan data sekunder, maka pengumpulan data tidak dilakukan melalui survei, wawancara, atau observasi lapangan, melainkan melalui seleksi literatur yang relevan dan kredibel.

Langkah pertama adalah identifikasi literatur. Peneliti melakukan pencarian literatur menggunakan basis data akademik seperti Google Scholar, Scopus, JSTOR, dan ScienceDirect untuk memperoleh artikel ilmiah dan buku yang berkaitan dengan tema penelitian, khususnya kepemimpinan digital, doktrin pertahanan, dan keamanan siber. Selain itu, penelusuran juga dilakukan pada situs resmi lembaga pertahanan negara terkait, misalnya Departemen Pertahanan Amerika Serikat (DoD), Kementerian Pertahanan Federasi Rusia (MoD), serta Israel Defense Forces (IDF).

Langkah kedua adalah seleksi literatur. Dari hasil penelusuran awal, hanya literatur yang memenuhi kriteria tertentu yang dipilih, yaitu: (1) relevan dengan topik penelitian, (2) diterbitkan oleh lembaga kredibel atau jurnal akademik bereputasi, (3) memuat data mutakhir (terutama dalam rentang 5–10 tahun terakhir), dan (4) memiliki keterkaitan langsung dengan aspek kepemimpinan digital, doktrin pertahanan, maupun kebijakan siber nasional. Dengan menggunakan kriteria ini,

penelitian dapat meminimalisasi bias dan meningkatkan kualitas data yang digunakan.

Langkah ketiga adalah klasifikasi data. Literatur yang telah terseleksi dikelompokkan ke dalam beberapa kategori utama: (a) literatur terkait doktrin pertahanan Rusia, Amerika Serikat, dan Israel; (b) literatur mengenai konsep kepemimpinan digital dan pengelolaan sumber daya teknologi; (c) literatur tentang kebijakan keamanan siber Indonesia. Proses klasifikasi ini bertujuan untuk memudahkan analisis perbandingan strategis serta penerapan pendekatan benchmarking dalam penelitian.

Langkah keempat adalah sintesis data awal, yaitu menyusun ringkasan isi literatur sesuai kategori yang telah ditentukan. Sintesis ini dilakukan dengan memperhatikan kata kunci, tema, serta perspektif analisis yang digunakan masing-masing sumber. Dengan cara ini, peneliti dapat membangun kerangka analisis yang konsisten untuk tahap analisis isi (content analysis), analisis komparatif, maupun analisis kebijakan pada bagian pembahasan.

Melalui tahapan pengumpulan data ini, penelitian memperoleh sumber informasi yang terarah, tervalifikasi, dan mampu memberikan dasar yang kuat untuk menjawab pertanyaan penelitian mengenai transformasi kepemimpinan digital dalam doktrin pertahanan, serta relevansinya bagi pembentukan doktrin pertahanan siber Indonesia.

#### 4. Teknik Analisis Data

Data yang terkumpul dalam penelitian ini dianalisis menggunakan kombinasi analisis isi (content analysis), studi perbandingan strategis (comparative strategic studies), serta analisis kebijakan (policy analysis). Pendekatan analitis ini dipilih untuk memahami pola kepemimpinan digital dalam doktrin pertahanan Rusia, Amerika Serikat, dan Israel, sekaligus merumuskan rekomendasi strategis bagi Indonesia.

Pertama, penelitian menggunakan analisis isi (content analysis) untuk menguraikan tema-tema utama dari literatur yang telah dikumpulkan. Setiap dokumen resmi, artikel akademik, maupun laporan think-tank dianalisis untuk menemukan konsep kunci seperti strategi kepemimpinan digital, pengelolaan sumber daya teknologi, model pertahanan siber, dan hubungan dengan keamanan nasional. Analisis isi ini memungkinkan peneliti untuk mengidentifikasi dimensi yang berulang, menyingkap makna implisit, dan menafsirkan arah kebijakan yang tersirat dalam literatur.

Kedua, data yang telah direduksi kemudian diproses dengan analisis perbandingan strategis. Analisis ini dilakukan dengan cara membandingkan pola kepemimpinan digital dalam doktrin pertahanan Rusia, Amerika Serikat, dan Israel pada beberapa indikator utama, yaitu: (1) struktur kepemimpinan dan tata kelola, (2) strategi penggunaan teknologi digital dan siber, (3) pengembangan sumber daya manusia, serta (4) integrasi dengan kepentingan keamanan nasional. Melalui pendekatan ini, dapat diidentifikasi persamaan, perbedaan, serta keunikan dari masing-masing negara.

Ketiga, penelitian menerapkan analisis kebijakan (policy analysis) dengan pendekatan siklus kebijakan (policy cycle). Tahapan analisis meliputi: (a) identifikasi masalah, yakni meningkatnya ancaman siber dan belum adanya doktrin pertahanan siber terpadu di Indonesia; (b) formulasi kebijakan, yaitu pembelajaran dari model Rusia, Amerika Serikat, dan Israel; (c) implementasi kebijakan, yakni kemungkinan strategi yang dapat diadopsi sesuai konteks Indonesia, misalnya pembentukan unit elit siber, kolaborasi multinasional, atau penguatan kedaulatan digital; serta (d) evaluasi kebijakan, yang memproyeksikan peluang dan tantangan implementasi doktrin pertahanan

siber di Indonesia.

Keempat, sebagai penguatan, penelitian ini menerapkan pendekatan benchmarking untuk menarik pelajaran dari praktik terbaik (best practices) global. Benchmarking dilakukan dengan membandingkan praktik unggul di Rusia (kontrol informasi strategis), Amerika Serikat (inovasi teknologi dan kolaborasi global), serta Israel (fleksibilitas kepemimpinan dan penguatan SDM). Dari hasil benchmarking, penelitian merumuskan elemen-elemen strategi yang paling relevan untuk diadaptasi oleh Indonesia dalam merumuskan doktrin pertahanan siber nasional.

Dengan demikian, kombinasi analisis isi, studi perbandingan strategis, analisis kebijakan, dan benchmarking menghasilkan kerangka analisis yang komprehensif. Pendekatan ini tidak hanya mendeskripsikan praktik di negara lain, tetapi juga mengkritisinya, menilai relevansinya, serta merumuskan rekomendasi kebijakan yang sesuai dengan konteks nilai, kebutuhan, dan keamanan nasional Indonesia.

## 5. Validitas Data

Validitas data dalam penelitian berbasis studi literatur ini dijaga melalui beberapa strategi yang memastikan keandalan, ketepatan, dan kredibilitas informasi yang dianalisis. Mengingat penelitian menggunakan sumber sekunder, maka pengujian validitas dilakukan dengan cara triangulasi sumber, evaluasi kredibilitas literatur, serta penguatan melalui benchmarking global.

Pertama, triangulasi sumber dilakukan dengan membandingkan data dari berbagai jenis literatur, meliputi artikel jurnal ilmiah, buku akademik, laporan lembaga internasional, dokumen resmi pemerintah, serta publikasi think-tank yang memiliki reputasi global. Dengan membandingkan berbagai sumber, penelitian dapat mengurangi bias dari satu perspektif tertentu dan memperoleh gambaran yang lebih objektif.

Kedua, evaluasi kredibilitas literatur diterapkan dengan menyeleksi sumber berdasarkan tingkat otoritas penerbit dan tahun publikasi. Hanya literatur dari jurnal terindeks, penerbit akademik bereputasi, atau lembaga resmi pertahanan dan keamanan negara yang digunakan sebagai rujukan utama. Selain itu, penelitian mengutamakan data terbaru (dalam kurun waktu 5–10 tahun terakhir) untuk memastikan relevansi dengan dinamika perkembangan teknologi dan keamanan siber.

Ketiga, penelitian menggunakan strategi verifikasi silang dengan cara mengonfirmasi informasi yang diperoleh dari satu sumber dengan sumber lain yang independen. Misalnya, kebijakan pertahanan siber Amerika Serikat tidak hanya dianalisis dari dokumen Department of Defense Cyber Strategy, tetapi juga diperbandingkan dengan analisis akademisi maupun laporan lembaga riset strategis seperti RAND Corporation.

Keempat, validitas diperkuat melalui pendekatan benchmarking global, yang membandingkan praktik kepemimpinan digital di Rusia, Amerika Serikat, dan Israel. Dengan menjadikan ketiga negara tersebut sebagai studi kasus pembanding, penelitian dapat menguji konsistensi data yang diperoleh sekaligus mengidentifikasi best practices yang terbukti efektif. Benchmarking ini berfungsi sebagai uji keabsahan internal (apakah data sejalan dengan temuan lintas kasus) dan uji keabsahan eksternal (apakah data relevan dengan konteks pertahanan Indonesia).

Dengan strategi validitas ini, penelitian tidak hanya mengandalkan satu sudut pandang, tetapi memadukan berbagai perspektif untuk memastikan hasil analisis memiliki dasar akademik yang kuat, objektif, serta dapat dipertanggungjawabkan secara ilmiah.

## HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa kepemimpinan digital dalam doktrin pertahanan memiliki pola yang berbeda di Rusia, Amerika Serikat, dan Israel, namun semuanya menegaskan urgensi pengelolaan sumber daya teknologi sebagai pilar keamanan nasional. Perbandingan ini memperlihatkan bahwa meskipun terdapat variasi strategi, terdapat benang merah berupa kebutuhan akan kepemimpinan digital yang kuat, integratif, dan berbasis nilai strategis.

### 1. Rusia: Sentralisasi dan Kedaulatan Digital

Kepemimpinan digital Rusia sangat dipengaruhi oleh tradisi politiknya yang menekankan pada kontrol negara dan sentralisasi kekuasaan. Konsep *Information Confrontation* yang dikembangkan sejak era Soviet masih menjadi kerangka utama dalam memandang ruang siber. Negara tidak hanya melihat siber sebagai instrumen pertahanan, tetapi juga sebagai alat untuk operasi ofensif, propaganda, dan perang informasi.

Peran lembaga keamanan seperti Federal Security Service (FSB) dan Main Directorate of the General Staff of the Armed Forces (GRU) sangat dominan dalam operasi siber. FSB berfokus pada keamanan domestik, termasuk pengawasan terhadap arus informasi di dalam negeri, sementara GRU lebih aktif dalam operasi ofensif di luar negeri. Roskomnadzor, lembaga pengawas media dan komunikasi, juga berperan besar dalam memastikan bahwa arus informasi domestik tetap terkendali sesuai dengan kepentingan negara.

Studi oleh Soldatov & Borogan (2020) menegaskan bahwa strategi siber Rusia bersifat state-centric. Negara menjadi aktor utama yang memobilisasi sumber daya teknologi, termasuk perusahaan teknologi domestik, untuk kepentingan strategis. Kasus serangan siber terhadap infrastruktur Ukraina pada 2014 dan 2022 menunjukkan bagaimana Rusia memanfaatkan kekuatan digital sebagai bagian dari strategi militer. Serangan ini tidak hanya melumpuhkan sistem energi dan komunikasi, tetapi juga menyebarkan disinformasi untuk melemahkan moral publik.

Bagi Indonesia, pelajaran penting dari Rusia adalah pentingnya konsistensi negara dalam memimpin kebijakan siber. Sentralisasi dapat memperkuat koordinasi, tetapi harus diimbangi dengan transparansi dan akuntabilitas agar tidak menimbulkan dominasi negara yang berlebihan terhadap ruang digital. Konsep information warfare yang diterapkan Rusia mengintegrasikan operasi militer konvensional dengan operasi informasi dan serangan siber. Pendekatan ini sejalan dengan pandangan Thomas (2019) bahwa Rusia memandang ruang informasi sebagai medan perang yang setara dengan darat, laut, dan udara. Implikasinya bagi Indonesia adalah pentingnya membangun kedaulatan digital melalui pengembangan infrastruktur domestik, peningkatan kemampuan deteksi dini serangan siber, dan pembentukan regulasi yang melindungi informasi strategis dari infiltrasi eksternal. Benchmarking dari Rusia menegaskan dua hal:

- Kekuatan:** kemampuan negara memobilisasi sumber daya digital secara terpusat untuk menghadapi ancaman eksternal.
- Kelemahan:** keterbatasan fleksibilitas karena kontrol ketat menghambat inovasi dan kolaborasi sektor swasta.

### 2. Amerika Serikat: Kolaborasi Multisektor dan Teknologi Mutakhir

Amerika Serikat mengadopsi pendekatan yang berbeda. Melalui U.S. Cyber Command (USCYBERCOM) dan Department of Defense (DoD), AS mengembangkan doktrin Defend Forward

yang berorientasi pada tindakan proaktif. Konsep ini berarti bahwa pertahanan siber tidak cukup hanya menunggu serangan, tetapi juga melibatkan operasi ofensif untuk melumpuhkan ancaman di luar negeri sebelum sampai ke dalam negeri. Strategi pertahanan siber Amerika, sebagaimana tertuang dalam Department of Defense Cyber Strategy (2018; 2023), menekankan pada pencegahan (deterrence), ketahanan (resilience), serta kerja sama internasional.

Karakteristik kepemimpinan digital ini tercermin dalam sinergi antara pemerintah, sektor swasta, akademisi, dan aliansi global. Hal ini sejalan dengan pendapat Nye (2020) yang menekankan pentingnya cyber power sebagai kombinasi antara kekuatan teknologi, regulasi, dan legitimasi global. Pembelajaran penting bagi Indonesia adalah perlunya mengembangkan ekosistem pertahanan siber yang inklusif, dengan melibatkan berbagai aktor non-negara seperti industri teknologi nasional, perguruan tinggi, dan komunitas riset.

Selain itu, AS mengembangkan arsitektur Zero Trust, yaitu pendekatan keamanan siber yang tidak lagi mengandalkan perimeter tradisional, melainkan mengasumsikan bahwa setiap jaringan sudah dalam kondisi rentan. Oleh karena itu, akses terhadap data dan sistem hanya diberikan berdasarkan otorisasi yang ketat, dengan pengawasan berlapis.

Peristiwa peretasan SolarWinds pada tahun 2020 dan serangan terhadap Colonial Pipeline pada 2021 menjadi titik balik penting bagi AS. Kedua kasus ini memperlihatkan kerentanan sektor swasta yang justru berperan vital dalam infrastruktur nasional. Sebagai respons, AS memperkuat kemitraan dengan perusahaan teknologi besar seperti Microsoft, Google, dan Amazon dalam mendeteksi, merespons, dan mencegah serangan siber. Model public-private partnership ini menjadi salah satu ciri khas kepemimpinan digital Amerika Serikat dalam bidang pertahanan. Benchmarking dari AS menunjukkan:

- a. **Kekuatan:** kapasitas inovasi tinggi melalui kolaborasi terbuka.
- b. **Kelemahan:** kerentanan akibat sistem yang terlalu bergantung pada aktor non-negara yang memiliki kepentingan komersial.

Bagi Indonesia, pelajaran yang dapat diambil adalah pentingnya melibatkan sektor swasta dan akademisi dalam merumuskan strategi pertahanan siber. Kolaborasi multisektor memungkinkan distribusi beban dan tanggung jawab yang lebih proporsional, sekaligus mempercepat inovasi teknologi yang relevan untuk pertahanan nasional.

### 3. Israel: Fleksibilitas dan Penguatan SDM Digital

Israel memandang kepemimpinan digital sebagai hasil dari fleksibilitas dan penguatan sumber daya manusia (SDM). Pembangunan kapasitas digital dilakukan sejak dulu melalui sistem pendidikan yang menekankan keterampilan teknologi, yang kemudian diarahkan untuk mendukung kebutuhan pertahanan. Unit elit seperti Unit 8200 menjadi contoh nyata keberhasilan integrasi antara inovasi militer dan ekosistem start-up teknologi sipil (Even, 2021).

Kepemimpinan digital Israel menekankan pada fleksibilitas, inovasi, dan pemanfaatan sumber daya manusia. Alih-alih hanya mengandalkan kekuatan negara, Israel menciptakan ekosistem yang memungkinkan sinergi antara militer, akademisi, dan sektor swasta. Hasilnya adalah percepatan inovasi teknologi yang dapat segera diintegrasikan ke dalam sistem pertahanan nasional.

Selain itu, Israel berhasil menunjukkan kemampuan pertahanan siber dalam menghadapi ancaman nyata, khususnya dari kelompok dan negara di kawasan Timur Tengah. Serangan siber

yang berasal dari Iran, Hamas, dan Hezbollah dijawab dengan respons cepat yang mengombinasikan teknologi pertahanan dengan operasi intelijen. Hal ini menunjukkan bahwa Israel mampu mengintegrasikan kepemimpinan digital dengan kebutuhan geopolitik regional.

Pendekatan ini menunjukkan bahwa keunggulan dalam pertahanan siber tidak hanya ditentukan oleh teknologi, tetapi juga oleh kualitas SDM yang mampu beradaptasi dengan cepat terhadap ancaman baru. Israel membuktikan bahwa investasi jangka panjang pada pendidikan teknologi, kewirausahaan digital, dan inkubasi inovasi dapat menghasilkan keunggulan strategis di ranah militer maupun sipil.

Pembelajaran penting bagi Indonesia adalah bahwa kemandirian pertahanan siber tidak mungkin dicapai tanpa strategi pengembangan SDM digital yang berkelanjutan. Indonesia perlu membangun kurikulum pendidikan yang menekankan literasi digital dan keamanan informasi sejak dini, memperkuat jejaring antara TNI, lembaga pendidikan, dan industri teknologi, serta menciptakan insentif bagi talenta digital agar berkontribusi pada pertahanan nasional. Selain itu, pembentukan unit khusus siber dengan kapasitas adaptif dapat menjadi langkah strategis untuk menghadapi ancaman yang dinamis. Benchmarking dari Israel memberi pelajaran bahwa ketahanan siber sangat bergantung pada kualitas manusia yang mampu beradaptasi dengan cepat terhadap perubahan ancaman. Fleksibilitas kepemimpinan menjadi faktor kunci keberhasilan, memungkinkan integrasi strategi militer dan sipil tanpa mengorbankan inovasi.

#### 4. Benchmarking dan Urgensi Doktrin Pertahanan Siber Indonesia

Dari ketiga studi kasus di atas, terlihat bahwa masing-masing negara memiliki model kepemimpinan digital yang unik. Rusia menekankan pada kontrol negara, Amerika Serikat mengedepankan kolaborasi multisektor, sedangkan Israel mengandalkan ekosistem inovasi berbasis sumber daya manusia. Benchmarking terhadap ketiganya memberikan wawasan penting bahwa tidak ada model tunggal yang dapat diadopsi secara penuh, melainkan perlu disesuaikan dengan kondisi sosial, politik, dan budaya Indonesia.

##### a. Benchmarking Global

**Rusia – Model Kedaulatan Digital** Rusia menekankan pada kontrol negara terhadap infrastruktur digital dan narasi informasi strategis. Hal ini lahir dari kebutuhan geopolitik Rusia untuk mengamankan ruang sibernya dari dominasi Barat. Pembelajaran bagi Indonesia adalah pentingnya membangun infrastruktur digital yang mandiri, mengurangi ketergantungan pada perangkat keras maupun perangkat lunak asing, serta membangun mekanisme regulasi untuk melindungi data strategis.

**Amerika Serikat – Model Kolaborasi Multisektor** Amerika Serikat menempatkan pertahanan siber sebagai upaya bersama antara pemerintah, swasta, akademisi, dan mitra internasional. Kekuatan utama model ini adalah inovasi teknologi melalui sektor swasta dan penguatan aliansi global. Indonesia dapat mengambil pelajaran berupa penguatan ekosistem pertahanan siber nasional yang kolaboratif serta memperluas diplomasi pertahanan siber di kawasan ASEAN dan Indo-Pasifik.

**Israel – Model SDM dan Inovasi Teknologi** Israel menonjol dalam pembangunan SDM unggul yang menjadi motor inovasi pertahanan digital. Pendekatan ini berfokus pada investasi jangka panjang dalam pendidikan, kewirausahaan digital, serta integrasi start-up teknologi dengan

kebutuhan militer. Indonesia dapat mengambil pelajaran strategis berupa prioritas pada penciptaan talenta digital nasional, pembentukan unit siber elit, dan pemanfaatan ekosistem teknologi lokal untuk mendukung pertahanan nasional.

#### b. Implikasi untuk Indonesia

Beberapa insiden besar dalam beberapa tahun terakhir menunjukkan bahwa Indonesia masih menghadapi kelemahan mendasar dalam keamanan siber. Kasus kebocoran data BPJS Kesehatan pada 2021, yang melibatkan lebih dari 279 juta penduduk, merupakan salah satu insiden terbesar di Asia Tenggara. Data yang bocor meliputi informasi sensitif seperti nomor KTP, alamat, dan status kepesertaan kesehatan, yang kemudian dijual di forum gelap (dark web). Kasus ini memperlihatkan lemahnya manajemen data, minimnya sistem enkripsi, serta kurangnya audit keamanan pada lembaga penyelenggara layanan publik.

Selanjutnya, pada Juli 2023, serangan terhadap Pusat Data Nasional (PDN) menimbulkan gangguan signifikan pada layanan publik, termasuk sistem imigrasi di bandara yang sempat lumpuh selama beberapa hari. Insiden ini tidak hanya mengganggu aktivitas masyarakat, tetapi juga mengurangi kepercayaan publik terhadap kemampuan negara dalam melindungi data dan layanan digital. Lebih jauh, peretasan PDN menyingkap kerentanan infrastruktur kritis serta kurangnya koordinasi lintas lembaga dalam menghadapi krisis siber.

Dua kasus ini menjadi cermin bahwa ancaman siber di Indonesia bukan lagi potensi, melainkan realitas. Jika dibandingkan dengan negara seperti Israel yang menempatkan keamanan digital sebagai prioritas nasional sejak dulu, Indonesia masih berada pada tahap awal dalam membangun ekosistem pertahanan siber yang solid. Oleh karena itu, penyusunan doktrin pertahanan siber berbasis kepemimpinan digital menjadi sangat mendesak, agar insiden serupa tidak berulang dengan dampak yang lebih besar terhadap stabilitas nasional.

Hasil benchmarking menunjukkan bahwa Indonesia membutuhkan doktrin pertahanan siber nasional yang memadukan unsur kedaulatan digital (Rusia), kolaborasi multisektoral (Amerika Serikat), dan penguatan SDM (Israel). Doktrin ini harus berbasis pada nilai Pancasila, kepentingan nasional, dan prinsip keamanan kolektif. Urgensi pembentukan doktrin pertahanan siber Indonesia didorong oleh beberapa faktor:

- 1) Meningkatnya ancaman siber lintas negara, seperti spionase digital, serangan terhadap infrastruktur kritis, dan propaganda siber.
- 2) Keterbatasan koordinasi antar lembaga nasional, yang berpotensi melemahkan respons terhadap ancaman siber.
- 3) Ketergantungan pada teknologi asing, yang menimbulkan kerentanan terhadap eksloitasi dan intervensi eksternal.
- 4) Kebutuhan akan SDM siber yang adaptif dan inovatif, agar Indonesia tidak hanya menjadi konsumen teknologi, tetapi juga produsen solusi digital strategis.

Dengan doktrin pertahanan siber yang jelas, Indonesia dapat memastikan perlindungan infrastruktur vital, memperkuat daya saing digital, serta mewujudkan kepemimpinan digital nasional yang adaptif terhadap perkembangan geopolitik global.

Terdapat tantangan aktual pertahanan siber Indonesia. Indonesia menghadapi lanskap ancaman siber yang kompleks. Laporan BSSN (2022; 2023) mencatat peningkatan signifikan serangan siber, mulai dari ransomware, pencurian data pribadi, hingga propaganda digital.

Infrastruktur kritis seperti sektor energi, transportasi, dan keuangan menjadi target potensial yang apabila terganggu dapat melemahkan stabilitas nasional. Tantangan utama dapat dipetakan dalam tiga aspek:

- 1) **Infrastruktur**: ketergantungan tinggi pada teknologi asing (cloud global, perangkat keras, perangkat lunak) menciptakan kerentanan terhadap kontrol eksternal.
- 2) **Regulasi**: meski ada UU Perlindungan Data Pribadi (2022), kerangka hukum pertahanan siber nasional belum terintegrasi dalam doktrin militer.
- 3) **SDM**: defisit talenta digital masih besar. Laporan World Bank menunjukkan Indonesia membutuhkan jutaan talenta digital baru setiap tahun untuk mengejar transformasi digital.

Terdapat peluang strategis di Indonesia karena memiliki modal besar diantaranya; populasi digital terbesar keempat di dunia, dengan penetrasi internet yang terus meningkat, posisi geopolitik strategis sebagai negara kepulauan di jalur Indo-Pasifik, menjadikan pertahanan siber bagian penting dari doktrin maritim, kehadiran BSSN sebagai lembaga khusus yang dapat berkolaborasi dengan TNI untuk membangun *Cyber Defense Command*. Adapun arah kebijakan pertahanan siber Indonesia merujuk pada benchmarking, arah kebijakan Indonesia perlu menekankan tiga pilar yaitu; yang pertama adalah **Kedaulatan Digital** (lesson from Russia): pembangunan *sovereign cloud*, data center domestik, dan regulasi infrastruktur kritis yang menempatkan negara sebagai pengendali utama. Kedua adalah **Kolaborasi Multisektor** (lesson from US) dengan memperkuat kerja sama pemerintah, industri teknologi, universitas, dan komunitas keamanan siber untuk mempercepat inovasi. Ketiga adalah **Penguatan SDM Digital** (lesson from Israel) dengan membangun ekosistem pendidikan teknologi sejak sekolah dasar, memperluas program pelatihan siber militer-sipil, serta menciptakan insentif bagi talenta digital untuk berkontribusi pada pertahanan nasional.

Merujuk pada benchmarking, Adapun arah kebijakan Indonesia perlu menekankan tiga pilar yaitu; **Kedaulatan Digital** (lesson from Russia): pembangunan *sovereign cloud*, data center domestik, dan regulasi infrastruktur kritis yang menempatkan negara sebagai pengendali utama, **Kolaborasi Multisektor** (lesson from US): memperkuat kerja sama pemerintah, industri teknologi, universitas, dan komunitas keamanan siber untuk mempercepat inovasi, dan **Penguatan SDM Digital** (lesson from Israel): membangun ekosistem pendidikan teknologi sejak sekolah dasar, memperluas program pelatihan siber militer-sipil, serta menciptakan insentif bagi talenta digital untuk berkontribusi pada pertahanan nasional. Berdasarkan hasil benchmarking dan analisis kebijakan, terdapat sejumlah implikasi strategis yang perlu dipertimbangkan dalam perumusan doktrin pertahanan siber Indonesia:

Pertama, doktrin pertahanan siber harus diposisikan sebagai bagian integral dan sejajar dengan doktrin pertahanan konvensional. Hal ini penting mengingat ancaman siber tidak lagi bersifat komplementer, melainkan telah menjadi dimensi utama yang menentukan efektivitas sistem pertahanan negara.

Kedua, diperlukan pembentukan unit militer khusus dengan mandat yang jelas, setara dengan *Cyber Command* di Amerika Serikat, guna mengoordinasikan operasi pertahanan siber lintas matra secara terpusat. Unit ini harus memiliki kewenangan strategis, sumber daya manusia terlatih, serta dukungan anggaran yang memadai agar mampu merespons ancaman siber secara proaktif dan berkesinambungan.

Ketiga, pembentukan *cyber reserve force* atau komponen cadangan digital dapat menjadi strategi inovatif untuk memperluas kapasitas pertahanan negara. Keterlibatan akademisi, profesional teknologi informasi, serta komunitas keamanan siber dalam komponen cadangan akan memperkuat ketahanan digital nasional dan memungkinkan negara menghadapi serangan skala besar dengan cepat.

Keempat, integrasi nilai-nilai Pancasila dan prinsip kedaulatan nasional dalam doktrin pertahanan siber menjadi pembeda *fundamental* Indonesia dibanding negara lain. Pendekatan ini tidak hanya berfokus pada perlindungan infrastruktur digital dan kepentingan ekonomi, tetapi juga memastikan bahwa ruang siber dikelola sesuai dengan jati diri bangsa dan diarahkan untuk menjaga keutuhan ideologi, kedaulatan, serta keamanan nasional secara holistik.

## KESIMPULAN

Penelitian ini menegaskan bahwa transformasi kepemimpinan digital dalam doktrin pertahanan merupakan kebutuhan strategis yang tidak dapat ditunda oleh Indonesia di tengah meningkatnya eskalasi ancaman siber global. Studi perbandingan terhadap Rusia, Amerika Serikat, dan Israel memperlihatkan bahwa model kepemimpinan digital dalam pertahanan siber dipengaruhi oleh faktor geopolitik, kapasitas teknologi, serta arah kebijakan nasional. Rusia menunjukkan kepemimpinan terpusat dengan orientasi pada kedaulatan digital dan kontrol negara, Amerika Serikat menekankan kolaborasi multisektor dan strategi *defend forward*, sementara Israel membangun ekosistem pertahanan siber adaptif yang berpusat pada sumber daya manusia melalui sinergi antara militer, industri, dan komunitas teknologi.

Dari perbandingan tersebut, terdapat tiga pelajaran penting bagi Indonesia. Pertama, perlunya doktrin pertahanan siber yang bersifat integratif, meliputi perlindungan infrastruktur kritis, pembangunan kapasitas digital, serta kolaborasi lintas sektor. Kedua, doktrin tersebut harus menempatkan penguatan sumber daya manusia digital sebagai prioritas utama, mengingat talenta siber merupakan fondasi keberlanjutan strategi pertahanan di era digital. Ketiga, doktrin pertahanan siber Indonesia harus berpijak pada kedaulatan digital yang berlandaskan nilai-nilai Pancasila, sehingga tidak sekadar bersifat teknis, tetapi juga memperkuat identitas nasional.

Secara filosofis, kepemimpinan digital dalam pertahanan bukan hanya isu teknologi, melainkan refleksi paradigma keamanan negara. Dalam perspektif realisme, pertahanan siber adalah instrumen kekuasaan negara dalam kompetisi global, sementara dalam perspektif konstruktivisme, doktrin pertahanan siber Indonesia harus dibangun berdasarkan nilai-nilai nasional serta konstruksi sosial-politik bangsa. Dengan demikian, doktrin pertahanan siber Indonesia bukan sekadar meniru praktik global, tetapi merupakan inovasi normatif yang menempatkan ruang siber sebagai arena pertahanan sekaligus diplomasi.

Implikasi praktis dari penelitian ini adalah urgensi pembentukan struktur kelembagaan pertahanan siber yang jelas dan terintegrasi, misalnya melalui pembentukan *Cyber Defense Command* di bawah TNI, serta pembangunan *cyber reserve force* yang melibatkan akademisi, komunitas teknologi, dan sektor swasta. Selain itu, kerja sama regional, khususnya melalui ASEAN *Cyber Defense Network*, menjadi langkah penting dalam memperkuat ketahanan kolektif menghadapi ancaman lintas batas.

Penting pula ditekankan bahwa penyusunan doktrin pertahanan siber Indonesia tidak hanya

menyangkut aspek teknis dan militer, tetapi juga nilai dan etika. Doktrin ini harus mampu menjawab isu-isu fundamental seperti kedaulatan data, perlindungan privasi, serta pencegahan penyalahgunaan teknologi yang berpotensi mengancam demokrasi. Di samping itu, literasi siber bagi masyarakat luas menjadi fondasi yang tidak kalah penting, karena pertahanan siber yang kuat hanya dapat terwujud melalui keterlibatan ekosistem kolaboratif antara pemerintah, sektor swasta, akademisi, dan masyarakat sipil.

Dengan demikian, pembentukan doktrin pertahanan siber Indonesia bukan lagi pilihan, melainkan keharusan untuk menjaga kedaulatan digital, memperkuat pertahanan nasional, dan membangun kepemimpinan digital yang adaptif, visioner, serta berkelanjutan. Doktrin ini harus hadir sebagai kombinasi antara strategi militer, kebijakan publik, inovasi teknologi, dan nilai-nilai kebangsaan yang berakar pada Pancasila. Melalui pendekatan tersebut, Indonesia dapat menjadi teladan dalam membangun ekosistem digital yang aman, etis, dan berdaulat, sekaligus memberikan kontribusi akademis maupun praktis dalam diskursus pertahanan dan keamanan siber di tingkat global.

## Daftar Pustaka

- ASEAN Secretariat. (2021). *ASEAN Cybersecurity Cooperation Strategy 2021–2025*. Jakarta: ASEAN Secretariat. Retrieved from <https://asean.org>
- Avolio, B. J., & Kahai, S. S. (2003). Adding the “E” to E-Leadership: How it may impact your leadership. *Organizational Dynamics*, 31(4), 325–338. [https://doi.org/10.1016/S0090-2616\(02\)00133-X](https://doi.org/10.1016/S0090-2616(02)00133-X)
- Avolio, B. J., Sosik, J. J., Kahai, S. S., & Baker, B. (2014). E-leadership: Re-examining transformations in leadership source and transmission. *The Leadership Quarterly*, 25(1), 105–131. <https://doi.org/10.1016/j.leagua.2013.11.003>
- Badan Siber dan Sandi Negara (BSSN). (2022). *Laporan Tahunan BSSN 2022: Keamanan Siber untuk Ketahanan Nasional*. Jakarta: BSSN.
- Badan Siber dan Sandi Negara (BSSN). (2023). *Laporan Tahunan BSSN 2023: Keamanan Siber untuk Ketahanan Nasional*. Jakarta: BSSN.
- Bass, B. M. (1990). From transactional to transformational leadership: Learning to share the vision. *Organizational Dynamics*, 18(3), 19–31. [https://doi.org/10.1016/0090-2616\(90\)90061-S](https://doi.org/10.1016/0090-2616(90)90061-S)
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder: Lynne Rienner Publishers.
- Connell, M., & Vogler, S. (2017). *Russia’s approach to cyber warfare*. Army Cyber Institute at West Point. Retrieved from <https://cyberdefensereview.army.mil>
- Cybersecurity Ventures. (2022). *Cybercrime To Cost The World \$10.5 Trillion Annually By 2025*. Cybersecurity Ventures Report. Retrieved from <https://cybersecurityventures.com>
- Department of Defense. (2018). *Department of Defense Cyber Strategy*. Washington, DC: U.S. Government Publishing Office.
- Department of Defense. (2023). *2023 Cyber Strategy Summary*. Washington, DC: U.S. Government Publishing Office.
- Even, S. (2021). Cybersecurity and national defense: Israel’s evolving doctrine. *Journal of Strategic Security*, 14(2), 45–63. <https://doi.org/10.5038/1944-0472.14.2.1920>
- Heifetz, R. A. (1994). *Leadership without easy answers*. Harvard University Press.
- International Telecommunication Union. (2021). *Global Cybersecurity Index 2020: Measuring commitment to cybersecurity*. International Telecommunication Union. <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021>

- Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace*. New York: Penguin Press.
- Morgenthau, H. J. (1948). *Politics among nations: The struggle for power and peace*. New York: Alfred A. Knopf.
- Nye, J. S. (2004). *Soft power: The means to success in world politics*. New York: Public Affairs.
- Nye, J. S. (2020). Power and interdependence in the age of information. *Foreign Affairs*, 99(2), 18–25.
- Pratama, A. (2022). *Keamanan Siber dan Kedaulatan Digital Indonesia*. Jakarta: Prenadamedia Group.
- Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux.
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.
- Tabansky, L., & Ben-Israel, I. (2015). *Cybersecurity in Israel*. Springer. <https://doi.org/10.1007/978-3-319-20499-4>
- Thomas, T. L. (2019). Russia's information warfare strategy: Can the nation cope in future conflicts? *Journal of Slavic Military Studies*, 32(3), 331–356. <https://doi.org/10.1080/13518046.2019.1645939>
- Waltz, K. N. (1979). *Theory of international politics*. Reading, MA: Addison-Wesley.
- Wendt, A. (1992). Anarchy is what states make of it: The social construction of power politics. *International Organization*, 46(2), 391–425. <https://doi.org/10.1017/S0020818300027764>