Literasiana
Jurnal Literasi Informasi Perpustakaan

Volume 1, Nomor 1, 30 Maret 2025
https://publikasiilmiah.unwahas.ac.id/literasiana
http://dx.doi.org/ 10.31942/

LITERASI DIGITAL : CYBER SECURITY SEBAGAI FONDASI KETAHANAN NASIONAL

Oleh

M. Fakhrudin, Najmud Daffa Hibatullah, Dr. Suparmi, S.IP., M.Pd.

Abstrak

Perkembangan pesat teknologi digital telah secara fundamental mengubah lanskap ancaman negara, menempatkan keamanan siber dan ketahanan nasional dalam hubungan yang tidak terpisahkan. Kajian literatur ini menganalisis sinergi krusial antara literasi digital (*soft power*) dan keamanan siber sebagai fondasi terintegrasi untuk Ketahanan Nasional Indonesia. Menggunakan metode kualitatif deskriptif dengan sintesis kritis terhadap 20 artikel jurnal ilmiah terbaru (2022 - 2025). Hasilnya didapatkan bahwa ketahanan Nasional Indonesia di era digital dapat dicapai melalui model Resiliensi Siber Hibrida yang menekankan integrasi formal dua pilar utama. Keamanan siber model ini menyediakan kerangka teknis, regulasi, dan doktrinal. Literasi digital berfungsi sebagai benteng kognitif yang vital untuk memitigasi risiko akibat faktor manusia, khususnya dalam menghadapi ancaman nirmiliter seperti hoaks dan judi *online* yang merusak Pancagatra. Namun, tantangan utama yang dihadapi adalah ketiadaan doktrin siber yang komprehensif serta rendahnya kapabilitas kognitif di masyarakat. Oleh karena itu, dapat disimpulkan bahwa penguatan Ketahanan Nasional menuntut pergeseran paradigma dari pendekatan yang berpusat pada negara (*state centered*) menjadi integrasi yang berpusat pada rakyat (*people centered*), melalui pelaksanaan program literasi digital yang masif, terstruktur, dan diselaraskan secara doktrinal dengan strategi keamanan siber nasional.

Kata Kunci : Ketahanan Nasional, Keamanan Siber, Literasi Digital, Ancaman Non Militer, Ketahanan Hybrid

Abstract

The rapid development of digital technology has fundamentally changed the landscape of national resilience in an inseparable relationship. This literature review analyzes the crucial synergy between digital literacy (soft power) and cybersecurity as an integrated foundation for Indonesia's National Resilience. Using a descriptive qualitative method with critical synthesis of 20 recent scientific journal articles (2022 - 2025), the results show that Indonesia's national resilience in the digital era can be achieved through a Hybrid Cyber Resilience model that emphasizes the formal integration of two main pillars. This cybersecurity model provides a technical, regulatory, and doctrinal framework. Digital literacy serves as a vital cognitive fortress to mitigate risks caused by human factors, especially in facing non-military threats such as hoaxes and online gambling that undermine the Pancagatra. However, the main challenges faced are the absence of a comprehensive cyber doctrine and low cognitive capabilities in Society. Therefore, it can be concluded that strengthening National Resilience requires a paradigm shift from a state-centered approach to a people-centered integration, through the implementation of massive, structured digital literacy programs that are doctrinally aligned with the national cybersecurity strategy.

Keywords: National Resilience, Cyber Security, Digital Literacy, Non Military Threat, Hybrid Resilience

PENDAHULUAN

Ketahanan Nasional dipandang sebagai kondisi dinamis yang mencakup ketahanan di seluruh dimensi Pancagatra, mulai dari ideologi hingga pertahanan dan keamanan (Lestari & Hasyim, 2024). Penguatan kondisi ini merupakan kunci utama untuk mewujudkan visi pembangunan jangka panjang, khususnya menuju Indonesia Emas 2045 (Fanani et al., 2024). Perkembangan TIK telah mendorong Indonesia memasuki era transformasi digital, membuka domain siber sebagai ruang strategis baru yang menuntut pendekatan multidimensional untuk mengatasi tantangan keamanan siber (Syawaluddin et al., 2025). Ancaman di ruang siber kini berevolusi menjadi risiko strategis yang mengancam fondasi Ketahanan Nasional secara sistemik, meluas dari serangan teknis seperti insiden *ransomware* pada PDSN yang mengungkap kelemahan infrastruktur dan SDM (Syawaluddin et al., 2025). Serangan menyasar pertahanan non-teknis masyarakat, termasuk penyebaran disinformasi, kebocoran data serta fenomena darurat judi *online* yang merusak pilar Pancagatra (Herawati et al., 2025). Oleh karena itu, pertahanan negara di era digital menuntut mobilisasi sumber daya nasional secara menyeluruh yang mengambil pembelajaran strategis dari pendekatan perang total (Widjayanto et al., 2025) Untuk memastikan resiliensi, dua pilar utama keamanan siber dan literasi digital harus menjadi fokus utama dalam perumusan kebijakan strategis.

Literasi digital sebagai dimensi *soft power* dan keamanan siber harus beroperasi secara sinergis untuk mencapai Ketahanan Nasional yang holistik. Ancaman siber yang bersifat kompleks menuntut pendekatan strategis multidimensional, khususnya melalui mekanisme diplomasi siber. Strategi diplomatik ini mensyaratkan integrasi pendekatan *multilateral, bilateral, dan multistakeholder* guna mengatasi ancaman siber lintas batas secara efektif. Literasi digital diidentifikasi sebagai strategi pertahanan dan pencegahan *cybercrime* yang efektif, sebab secara empiris, kerentanan individu dan organisasi terhadap kejahatan siber banding lurus dengan rendahnya literasi digital (Ramadhany et al., 2025). Kerangka kompetensi seperti *Digital Competence Framework* digunakan untuk mengukur penguasaan literasi digital yang esensial dalam membentuk Resiliensi Informasi (*Information Resilience*) kemampuan untuk bertahan dari misinformasi dan disinformasi (Sonni et al., 2025). Resiliensi informasi masih terkendala oleh adanya *gap* antara narasi media mengenai kecanggihan teknologi seperti *Artificial Intelligence* (AI) sebagai solusi misinformasi dengan pemahaman kritis publik.

Keamanan siber merepresentasikan pertahanan yang fokus pada kesiapan teknis, kelembagaan, dan regulasi. Meskipun demikian, sektor ini masih menghadapi tantangan besar, terutama pada aspek hukum terkait implementasi UU ITE serta ketiadaan doktrin siber yang

komprehensif (Siber & Sandi, 2022). Keterbatasan ini mengharuskan negara memperkuat fondasi pertahanan siber melalui pembentukan doktrin, optimalisasi tata kelola intelijen siber, peningkatan SDM, serta regulasi hukum (Setiadi et al., 2025). Literasi digital berfokus pada kapabilitas dan resiliensi kognitif Masyarakat untuk memperkuat fondasi ketahanan nasional. Masyarakat dengan literasi tinggi diidentifikasi sebagai kunci utama untuk membangun pertahanan efektif terhadap hoaks dan propaganda ideologis (Yahya et al., 2023). Namun, Indonesia masih menghadapi tantangan serius berupa rendahnya literasi digital dan *civic literacy* di Masyarakat (Ginting et al., 2025). Hal tersebut diperparah oleh adanya *gap* pemahaman publik mengenai peran teknologi seperti AI dalam melawan misinformasi (Sonni et al., 2025). Penguatan literasi digital harus diintegrasikan melalui strategi pendidikan kontekstual didukung peran pendidikan pertahanan (Sujana et al., 2024). *Cyber security* merepresentasikan pertahanan yang fokus pada kesiapan teknis, kelembagaan, dan regulasi. Berbagai upaya telah dilakukan tetapi tantangan dalam aspek ini masih besar. Salah satunya adalah masalah hukum, dimana implementasi UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) menghadapi keterbatasan cakupan hukum, kapasitas penegakan yang terbatas, dan sifat kejahatan siber yang bersifat transnasional (Maisaroh et al., 2025). Keterbatasan ini mengharuskan negara untuk memperkuat fondasi pertahanan siber melalui pendekatan yang lebih terstruktur.

Langkah-langkah strategis dalam penguatan *cyber security* sangat krusial. Salah satunya adalah kebutuhan mendesak untuk membentuk doktrin pertahanan siber Indonesia, mengambil pembelajaran strategis dari transformasi kepemimpinan digital dan strategi pertahanan siber di negara maju seperti Rusia, Amerika Serikat, dan Israel (Siber & Sandi, 2022). Selain itu, tata kelola intelijen siber juga harus dioptimalkan untuk menghadapi tantangan strategis yang kompleks (Mudra & Prasidya, 2024). Penguatan juga harus mencakup sisi regulasi, seperti optimalisasi fungsi Jaringan Dokumentasi dan Informasi Hukum Nasional (JDIHN) dalam menjamin keautentikan informasi hukum untuk Ketahanan Hukum Nasional (Setiadi et al., 2025). Semua upaya ini akan gagal tanpa adanya peningkatan kapasitas dan kesadaran Sumber Daya Manusia (SDM) sebagai benteng pertahanan teknis di berbagai institusi, termasuk di platform media sosial (Wahyudi et al., 2025). Literasi digital berfungsi sebagai dimensi *soft power* yang berfokus pada kapabilitas dan resiliensi kognitif Masyarakat yang diidentifikasi sebagai kunci utama dalam membangun pertahanan yang efektif terhadap penyebaran hoaks dan disinformasi (Yahya et al., 2023). Mayarakat dengan literasi tinggi mampu memilah informasi dan berpikir kritis, sehingga menjadi benteng pertahanan pertama melawan ancaman ideologis dan propaganda yang mengancam persatuan bangsa (Lestari & Hasyim, 2024).

Indonesia masih menghadapi tantangan serius dalam aspek resiliensi digital, yaitu kemampuan bertahan dari ancaman masih terkendala oleh rendahnya literasi digital di tengah masyarakat (Ginting et al., 2025). Selain itu, rendahnya literasi digital juga berimplikasi pada lemahnya pengetahuan terkait *civic literacy* di kalangan masyarakat yang menjadikan mereka rentan terhadap manipulasi informasi. Tantangan ini diperparah oleh adanya gap antara narasi media mengenai peran teknologi, seperti *Artificial Intelligence (AI)* dalam melawan misinformasi dengan pemahaman publik yang memadai (Sonni et al., 2025). Untuk mengatasi hal ini, penguatan literasi digital harus diintegrasikan melalui strategi pendidikan kontekstual di sekolah. Hal tersebut terbukti efektif meningkatkan keterampilan berpikir kritis, kedisiplinan, dan empati siswa dalam menghadapi ancaman siber (Maisaroh et al., 2025). Peran pendidikan pertahanan diperlukan untuk membangun kesadaran keamanan nasional di masyarakat dan meningkatkan kewaspadaan terhadap ancaman siber (Sujana et al., 2024).

Literasi digital dan keamanan siber adalah dua pilar yang saling memengaruhi dan harus beroperasi secara sinergis untuk mencapai ketahanan nasional yang optimal. *Cyber security* menyediakan infrastruktur dan kerangka regulasi, sementara literasi digital memastikan bahwa manusia sebagai titik terlemah dalam rantai keamanan siber memiliki kesadaran dan kemampuan kritis yang memadai. Isu kedaulatan data di Indonesia tidak dapat diselesaikan hanya dengan pendekatan *state centered* (kebijakan pemerintah), tetapi harus diimbangi dengan pendekatan *people centered*, yaitu peningkatan kapasitas dan kapabilitas warga negara dalam melindungi data pribadinya (Aji, 2022). Integrasi kedua pilar ini juga mendasari upaya bela negara dan penguatan Integritas Nasional. Literasi digital merupakan instrumen krusial dalam pertahanan kognitif karena internet sering digunakan untuk menyebarkan hoaks dan materi anti Pancasila yang merusak persatuan dan fondasi kebangsaan (Agung et al., 2022). Untuk membangun kesiapsiagaan kolektif ini, pendidikan pertahanan memiliki peran strategis. Pendidikan ini diposisikan sebagai pilar utama dalam Sistem Pertahanan Semesta yang bertujuan membentuk kesiapsiagaan sipil dan kesadaran kolektif masyarakat terhadap ancaman multidimensi, termasuk ancaman non-tradisional seperti radikalisasi digital (Tarom, 2025) .Oleh karena itu, sinergi antara kebijakan Keamanan Siber (aspek teknis dan diplomatik) dan program Literasi Digital (aspek kognitif dan edukatif melalui Pendidikan Pertahanan) adalah fondasi bagi model Ketahanan Nasional Hibrida yang adaptif dan tangguh di era digital.

Banyak kajian yang menyoroti urgensi masing-masing pilar sehingga terdapat *gap* dalam penelitian yang mensintesis kedua konsep utama ini sebagai fondasi tunggal dan terintegrasi bagi ketahanan nasional. Keberhasilan pertahanan siber tidak dapat diukur hanya dari canggihnya

teknologi atau lengkapnya regulasi, melainkan dari tingkat resiliensi seluruh sistem, termasuk *human factor*. Oleh karena itu, penelitian ini berupaya mengisi *gap* tersebut dengan menganalisis secara mendalam mekanisme pengintegrasian literasi digital sebagai *soft defense* dengan kebijakan keamanan guna merumuskan model ketahanan nasional yang holistik, tangguh, dan adaptif di era digital.

METODE PENELITIAN

Penelitian ini menerapkan pendekatan studi kepustakaan (*literature review*) yang dirancang secara sistematis untuk menghimpun, menilai, dan menganalisis berbagai sumber ilmiah yang berkaitan dengan konsep literasi digital, keamanan siber, dan ketahanan nasional. Penelusuran literatur dilakukan melalui layanan *Google Scholar* dan perangkat lunak *Publish or Perish* dengan menggunakan sejumlah kata kunci terkontrol, yaitu "literasi digital," "keamanan siber," "ketahanan nasional," dan "kapasitas masyarakat digital." Rentang pencarian dibatasi pada publikasi tahun 2020 hingga 2025 untuk menjamin keterbaruan data dan relevansi terhadap perkembangan ekosistem digital Indonesia. Dari proses pencarian awal, diperoleh 200 artikel ilmiah yang memenuhi kriteria umum relevansi. Seluruh artikel tersebut kemudian diseleksi secara bertahap melalui penyaringan tematik, penilaian kualitas publikasi, kesesuaian abstrak, serta kelengkapan naskah. Tahap penyaringan menghasilkan 40 artikel yang relevan secara substantif, dan dari jumlah tersebut terdapat 20 artikel yang dapat diakses penuh serta layak dianalisis pada tahap berikutnya.

Proses analisis literatur dilakukan menggunakan analisis isi dan analisis tematik yang mencakup kegiatan membaca mendalam, pengkodean konsep, dan sintesis temuan berdasarkan konstruksi teoritis dan empiris yang termuat dalam publikasi terpilih. Seluruh artikel dikaji melalui identifikasi sistematis terhadap sejumlah aspek inti, antara lain: (1) definisi dan cakupan literasi digital dalam konteks masyarakat siber; (2) hubungan literasi digital dengan perilaku keamanan informasi individu; (3) pola ancaman siber yang relevan dengan konteks sosial Indonesia; serta (4) kontribusi literasi digital terhadap pembentukan ketahanan nasional. Artikel yang telah dianalisis kemudian dibandingkan satu sama lain untuk menemukan pola konsistensi maupun variasi temuan sehingga menghasilkan gambaran yang berimbang dan dapat dipertanggungjawabkan secara ilmiah. Validitas temuan dijamin melalui prosedur triangulasi sumber dan pemeriksaan silang terhadap keakuratan data pada dokumen asli. Dengan demikian, hasil penelitian yang diperoleh melalui metode ini memiliki tingkat kredibilitas dan reliabilitas yang tinggi serta mampu memberikan pemahaman komprehensif mengenai peranan literasi digital sebagai fondasi keamanan siber dalam memperkuat ketahanan nasional.

HASIL DAN PEMBAHASAN

Bagian hasil dan pembahasan ini merupakan tahap inti dari kajian literatur yang menyajikan sintesis kritis dari sejumlah artikel ilmiah terpilih yang telah lolos kriteria inklusi, fokus pada interkoneksi antara variabel literasi digital, *cyber security*, dan ketahanan nasional. Temuan literatur ini berfungsi sebagai data primer kualitatif yang mendasari analisis mendalam dalam upaya menjawab rumusan masalah yang berkaitan dengan urgensi sinergi pertahanan hibrida di Indonesia. Untuk mempermudah pemetaan argumen dan mengidentifikasi temuan kunci dari masing-masing studi sebagai basis data pembahasan, ringkasan hasil ekstraksi data literatur disajikan dalam bentuk tabel berikut.

Tabel 1. Ekstraksi Jurnal Terkait Literasi Digital*, Cyber Security*, dan Ketahanan Nasional

NNo	Peneliti dan Tahun	Subjek	Metode Penelitian	Hasil Penelitian
11	Syawaluddin, Putra, & Putra (2025)	*Cyber Security* & Ketahanan Nasional	Kualitatif, Deskriptif	Insiden siber (PDSN) menunjukkan kelemahan strategis pada infrastruktur, SDM, dan tata kelola regulasi, menegaskan keamanan siber sebagai prioritas nasional.
22	Herawati, Risdhianto, & Saptono (2025)	Ancaman Nirmiliter & Ketahanan Nasional	Kualitatif, *Literature Review*	Judi *online* diidentifikasi sebagai ancaman nirmiliter yang merongrong pilar Pancagatra secara sistemik, menuntut strategi pertahanan total.
33	Lestari (2024)	Literasi & Ketahanan Nasional (Ideologi)	Kualitatif	Literasi berfungsi sebagai benteng pertahanan ideologi dan keutuhan bangsa, menjadi *soft defense* pertama melawan serangan informasi menyesatkan.
44	Maharani & Atman (2025)	Strategi Nasional Keamanan Siber (SNKS)	Kualitatif, Analisis Konten	Diperlukan evaluasi komprehensif terhadap SNKS untuk menanggulangi ancaman dinamis seperti

				kebocoran data dan penyebaran disinformasi yang mengganggu stabilitas.
55	Aji (2022)	Kedaulatan Data & Cyber Security	Kualitatif, Ekonomi Politik	Perlindungan data siber harus mengintegrasikan pendekatan *state centered* (regulasi) dan *people centered* (kapabilitas warga) untuk efektivitas penuh.
66	Anshori & Hidayat (2023)	Literasi Informasi & Hoaks	Kualitatif	Penguatan literasi informasi adalah kunci utama pertahanan efektif terhadap penyebaran hoaks, meningkatkan resiliensi masyarakat.
77	Ginting, Arifyanto, & Ghafur (2025)	Resiliensi Digital & Literasi Digital	Kualitatif, Analisis Literatur	Resiliensi digital Indonesia terhambat oleh rendahnya tingkat literasi digital masyarakat, menekankan perlunya peningkatan kesadaran nasional.
88	Maisaroh, Sukriono, & Suhartono (2025)	Literasi Digital & Pendidikan Kontekstual	Kualitatif, Deskriptif	Penerapan strategi pendidikan kontekstual (berbasis kasus) terbukti efektif dalam meningkatkan keterampilan berpikir kritis dan literasi digital siswa.
99	Wahyudi, Sulistyowati, & Bikorin (2025)	SDM & Kesadaran Cyber Security	Kualitatif, *Abdimas*	Peningkatan kapasitas dan kesadaran SDM dalam pengamanan siber, khususnya pada platform media sosial, sangat krusial sebagai titik lemah dalam sistem keamanan.

Ketahanan nasional di era digital telah bergeser dari konsep pertahanan tradisional menjadi kebutuhan akan resiliensi hibrida yang memadukan pertahanan teknis dan kognitif. Sinergi antara *cyber security* (teknologi dan regulasi) dan literasi digital sebagai pilar *soft power* (kesadaran dan kapabilitas individu) merupakan imperatif strategis, bukan sekadar pilihan kebijakan. Secara formal, *cyber security* menyediakan kerangka perlindungan infrastruktur vital negara. Namun, temuan menunjukkan bahwa kegagalan infrastruktur seringkali diperparah oleh kelemahan pada *human factor*, seperti yang dicontohkan oleh insiden serangan pada PDSN (Syawaluddin et al., 2025). Titik kelemahan ini hanya dapat ditutup oleh literasi digital. Literasi digital memastikan bahwa individu (SDM di institusi atau warga negara) memiliki kesadaran dan kehati-hatian yang memadai, misalnya dalam mengelola keamanan media sosial, yang terbukti krusial dalam pencegahan kebocoran informasi (Wahyudi et al., 2025).

Sinergi ini terlihat jelas dalam dimensi ancaman nirmiliter. Ancaman siber tidak hanya berbentuk serangan teknis, tetapi juga serangan ideologis dan sosial, seperti penyebaran hoaks dan judi *online* (Herawati et al., 2025). Literasi digital dalam konteks ini berfungsi sebagai benteng pertahanan ideologi yang krusial, meningkatkan kemampuan individu dalam menyaring informasi, sehingga mereka tidak mudah terprovokasi atau menjadi korban manipulasi digital (Lestari & Hasyim, 2024). Hal ini menguatkan argumentasi bahwa perlindungan siber tidak dapat mengandalkan pendekatan *state centered* semata, melainkan wajib diimbangi dengan peningkatan kapasitas *people centered* (Aji, 2022). Oleh karena itu, sinergi dan membentuk mekanisme pertahanan dua lapis yaitu lapisan teknis institusional dan lapisan kognitif-sosial, yang secara bersamaan menjamin stabilitas ketahanan nasional. Meskipun urgensi sinergi telah terbukti, proses integrasi *cyber security* dan literasi digital menghadapi tantangan signifikan, baik pada level tata kelola negara maupun budaya masyarakat. Pada aspek kelembagaan, tantangan utama berpusat pada ketiadaan kerangka doktrin pertahanan siber yang komprehensif. Studi perbandingan menunjukkan bahwa negara maju memiliki doktrin yang jelas, yang menjadi basis bagi transformasi kepemimpinan digital dan penguatan pertahananan (Hal et al., 2025). Ketiadaan doktrin ini menciptakan *gap* dalam penyelarasan kebijakan lintas sektor dan menghambat integrasi program literasi digital ke dalam rantai komando keamanan.

Selain itu, regulasi yang ada, seperti UU ITE terbukti memiliki keterbatasan, baik dari cakupan hukum yang sempit maupun kapasitas penegakan yang tidak mampu mengimbangi sifat kejahatan siber yang transnasional (Maisaroh et al., 2025). Tantangan ini diperparah oleh perlunya evaluasi Strategi Nasional Keamanan Siber (SNKS) secara terus-menerus agar dapat merespons ancaman dinamis, termasuk isu-isu terkait kebocoran data dan disinformasi (Maharani et al., 2025). Tanpa kerangka hukum dan doktrinal yang kuat dan adaptif, upaya peningkatan Literasi

Digital akan berjalan sporadis dan tidak memiliki dukungan institusional yang memadai.

Tantangan dari sisi masyarakat berakar pada rendahnya kapabilitas kognitif digital. Temuan menunjukkan bahwa Indonesia masih menghadapi tantangan besar dalam membangun resiliensi digital, yang secara langsung disebabkan oleh rendahnya tingkat literasi digital (Ginting et al., 2025). Rendahnya literasi ini tidak hanya sebatas ketidakmampuan teknis, tetapi juga berimplikasi pada lemahnya *Civic Literacy*, yang membuat masyarakat rentan terhadap manipulasi politik dan berita bohong . Meskipun terdapat upaya edukasi, masih ada kesenjangan antara narasi media dan pemahaman publik; misalnya, mengenai peran *Artificial Intelligence* (AI) dalam melawan misinformasi. Masyarakat belum sepenuhnya memiliki keterampilan kritis yang memadai untuk mengevaluasi konten yang dihasilkan teknologi canggih (Sonni et al., 2025). Oleh karena itu, tantangan budaya ini menuntut perubahan mendasar dalam strategi pendidikan, yakni perlunya pendekatan kontekstual dan berbasis kasus untuk menanamkan keterampilan berpikir kritis dan empati digital sejak dini .

Berdasarkan analisis sinergi dan tantangan, penelitian ini merumuskan "Model Ketahanan Nasional Digital Integratif" yang bertumpu pada interaksi simbiotik antara Literasi Digital dan cyber security. Model ini menggarisbawahi pergeseran paradigma dari pertahanan yang terpisah menjadi satu sistem perlindungan holistik. Model yang diusulkan adalah Resiliensi Siber Hibrida yang dicirikan oleh ketergantungan timbal balik antara empat komponen:

1. Pilar Regulasi & Institusi

   Negara wajib memastikan kerangka hukum dan kelembagaan yang kuat, termasuk evaluasi berkelanjutan terhadap SNKS dan pembentukan doktrin pertahanan siber sebagai cetak biru kebijakan (Maharani et al., 2025).

2. Pilar Infrastruktur & Teknis

   Fokus pada penguatan infrastruktur vital, sistem keamanan data, dan peningkatan kapasitas SDM profesional siber (Syawaluddin et al., 2025).

3. Pilar Kognitif & Pendidikan

   Melalui pendidikan formal dan non-formal, menanamkan kemampuan berpikir kritis, *digital hygiene*, dan *civic literacy* (Maisaroh et al., 2025).

4. Pilar Kesadaran & Kebangsaan

   Integrasi literasi digital dengan pendidikan pertahanan untuk membangun kesadaran keamanan nasional di tengah masyarakat (Sujana et al., 2024).

Literasi digital bertindak sebagai model mekanisme mitigasi risiko manusia dengan

meningkatkan kesadaran, secara preventif mengurangi keberhasilan serangan berbasis rekayasa sosial (*social engineering*) yang menjadi titik lemah utama sistem ketahanan nasional. Sebaliknya, *cyber security* berfungsi sebagai penjamin lingkungan digital yang aman untuk pelaksanaan literasi digital, menyediakan platform edukasi dan regulasi perlindungan data yang kredibel (Aji, 2022). Ketahanan nasional tidak hanya terjamin dari serangan teknis *hacker*, tetapi juga dari erosi ideologi dan fragmentasi sosial yang disebabkan oleh serangan nirmiliter, seperti yang ditimbulkan oleh judi *online* (Herawati et al., 2025). Model ini menekankan bahwa pertahanan sejati di era digital terletak pada kolaborasi *state centered* dan *people centered* yang terstruktur.

KESIMPULAN

Penelitian ini bertujuan menganalisis sinergi antara literasi digital dan *cyber security* sebagai fondasi terintegrasi bagi ketahanan nasional di tengah kompleksitas ancaman digital. Berdasarkan analisis kualitatif terhadap literatur ilmiah terbaru, ditemukan bahwa ketahanan nasional di era digital merupakan hasil dari pertahanan hibrida yang tidak dapat dipisahkan. *Cyber security* menyediakan infrastruktur, kebijakan, dan doktrin pertahanan teknis, sementara literasi digital berfungsi sebagai dimensi *soft power* yang sangat krusial, bertindak sebagai benteng kognitif (*cognitive defense*) dan mekanisme mitigasi risiko manusia terhadap ancaman nirmiliter yang merongrong fondasi Pancagatra. Sinergi ini wajib diimplementasikan melalui pendekatan *people centered* untuk melengkapi upaya *state centered* dalam perlindungan data dan kedaulatan siber .

Implementasi sinergi ini menghadapi dua tantangan utama yaitu tantangan kelembagaan yang ditandai dengan ketiadaan doktrin pertahanan siber yang komprehensif dan keterbatasan regulasi serta tantangan sosial berupa rendahnya resiliensi dan kapabilitas kognitif masyarakat akibat tingkat literasi digital yang belum memadai. Oleh karena itu, penelitian ini merumuskan Model Resiliensi Siber Hibrida. Model ini menekankan perlunya integrasi formal program penguatan literasi digital melalui pendidikan kontekstual yang menanamkan berpikir kritis dengan inisiatif *cyber security* melalui peningkatan kapasitas SDM dan evaluasi berkelanjutan terhadap Strategi Nasional Keamanan Siber (SNKS). Penguatan sinergis literasi digital adalah prasyarat fundamental untuk mewujudkan ketahanan nasional yang tangguh dan adaptif, sehingga menjamin tercapainya visi Indonesia Emas 2045. Rekomendasi strategis diarahkan pada pembentukan doktrin siber yang mengikat seluruh kementerian/lembaga dan menjadikan peningkatan Literasi Digital sebagai komponen wajib dalam Pendidikan Pertahanan

DAFTAR PUSTAKA

Agung, A., Candra, M., & Islam, N. (2022). *Digital Literacy as an Effort to Build National Resilience*. *1*(3), 1–9.

Aji, M. P. (2022). *Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective*. https://doi.org/10.22212/jp.v13i2.3299

Fanani, A., Midhio, I. W., & Hendra, A. (2024). *TANTANGAN PERTAHANAN NASIONAL MENUJU INDONESIA EMAS 2045*. *5*(4), 379–391.

Ginting, R. G., Arifyanto, G. T., & Ghafur, F. (2025). *Defending The State in The Digital Domain : Between Cyber Threats and National Awareness*.

Hal, M., Ardiani, G. T., Saefullah, A., Andrian, R. N. R., & Sudaryanti, D. S. (2025). *DHIGANA : Jurnal Pengabdian Kepada Masyarakat Bidang Ilmu Manajemen Bela Negara di Dunia Maya : Jaga Data , Jaga Bangsa (Cyber Patriotism : Protect Data , Protect the Nation) Konsep bela negara*. *3*(1).

Herawati, D. A., Risdhianto, A., & Saptono, E. (2025). *INDONESIA DARURAT JUDI ONLINE : JUDI ONLINE SEBAGAI ANCAMAN NIRMILITER TERHADAP*. *5*(5), 1251–1261. https://doi.org/10.53866/jimi.v5i5.991

Wahyudi, I., Sulistyowati, A., & Bikorin. (2025). *Jurnal Abmas*. *25*(1), 29–38.

Lestari, S., & Hasyim, U. W. (2024). *PENTINGNYA LITERASI DALAM MENJAGA KEUTUHAN DAN*. *1*.

Maharani, M. A., Atman, W., Ilmu, D., & Internasional, H. (2025). *Evaluasi Strategi Nasional Keamanan Siber Indonesia dalam Menanggapi Ancaman Digital Indonesia Keamanan Siber sebagai Bagian dari Keamanan Nasional*.

Maisaroh, A. A., Sukriono, D., & Suhartono, E. (2025). *Optimalisasi Literasi Digital dalam Materi Pertahanan dan Keamanan : Strategi Pendidikan Kontekstual di Sekolah*. *14*(2), 2181–2194.

Mudra, C., & Prasidya, F. G. (2024). *Jurnal Kajian Stratejik Ketahanan Nasional Cybersecurity dan Tata Kelola Intelijen Cybersecurity dan Tata Kelola Intelijen*. *7*(1). https://doi.org/10.7454/jkskn.v7i1.10086

Ramadhany, A. F., Damayanti, N. E., & Rahmania, L. A. (2025). *Digital Literacy as a Cyber Crime Defense and Prevention Strategy*. *2025*, 778–785. https://doi.org/10.11594/nstp.2025.47116

Setiadi, W., Hukum, F., Pembangunan, U., Labu, P., Selatan, J., Hukum, F., Pembangunan, U., Labu, P., Selatan, J., Junaidi, A. H., Pembinaan, B., Nasional, H., & Timur, J. (2025). *Optimizing the function of jdihn in ensuring the availability and authenticity of consolidated legal documentation and information for national legal resilience*. *14*, 253–270.

Siber, B., & Sandi, D. A. N. (2022). *STRATEGI INDONESIA MEMBENTUK CYBER SECURITY DALAM MENGHADAPI ANCAMAN CYBER CRIME MELALUI*. *7*(2), 295–316.

Sonni, A. F., Mau, M., & Akbar, M. (2025). *AI and Digital Literacy : Impact on Information Resilience in Indonesian Society*.

Sujana, D., Sukrisna, C., Purwaningsih, E., Teknis, P., Pertahanan, F., Kemhan, B., Teknis, P., Pertahanan, F., Kemhan, B., & Kemhan, S. B. (2024). *Peran Pendidikan Pertahanan dalam Membangun Kesadaran Keamanan Nasional di Masyarakat*. *2*(2), 62–72.

Syawaluddin, A. S., Surabaya, U. M., & Sutorejo, D. (2025). *CYBER SECURITY DAN KETAHANAN NASIONAL : TANTANGAN DAN SOLUSI DI ERA DIGITAL TANTANGAN DAN SOLUSI DI ERA DIGITAL*. *3*(6).

Tarom, M. (2025). *Peran Strategis Pendidikan Pertahanan dalam Penguatan Sistem Keamanan Nasional Indonesia*. *2*(1).

Widjayanto, J., Susetyo, E., & Leonardo, V. (2025). *Perang total dan mobilisasi*

sumber daya nasional dalam Perang Dunia II : Pembelajaran strategis bagi ketahanan nasional Indonesia Total war and the mobilization of national resources during World War II : Strategic insights for Indonesia ' s national resilience Abstrak. *8*(2), 441–451. https://doi.org/10.17977/um022v8i22025p441-451

Yahya, A., Pengajar, A., Ilmu, C., Nurohman, M. E., Pengajar, H., & Selomerto, N. S. (2023). *Membangun Pertahanan Terhadap Hoaks : Penguatan Literasi Informasi di Era Digital Oleh*. *1*, 1–15.