

National defense policy based on readiness against non-military threat

Setyo Hani Susanto¹, Asep Adang Supriyadi², and Faonaso Harefa³
^{1),2),3)}Universitas Pertahanan, Matraman, Jakarta Timur, Jakarta, Indonesia

Article Info

Article history

Received : Jul 09 2025

Revised : Jul 11, 2025

Accepted : Jul 22, 2025

Abstrak

Penelitian ini membahas urgensi implementasi dan penerapan sistem pertahanan rakyat semesta sebagai pendekatan adaptif dan strategis dalam memperkuat ketahanan nasional Indonesia di tengah ancaman multidimensi yang semakin kompleks dan dinamis. Ancaman terhadap keamanan negara saat ini tidak hanya berasal dari aspek militer yang bersifat fisik, tetapi juga mencakup serangan siber, disinformasi, pandemi, sabotase ekonomi, dan perubahan iklim. Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi pustaka terhadap literatur ilmiah, dokumen kebijakan pertahanan negara, serta praktik internasional. Hasil analisis menunjukkan bahwa implementasi pertahanan rakyat semesta di Indonesia masih menghadapi berbagai tantangan, seperti lemahnya koordinasi lintas sektor, tumpang tindih regulasi, keterbatasan anggaran, dan rendahnya literasi pertahanan masyarakat. Keberhasilan sistem ini sangat bergantung pada keterlibatan aktif seluruh elemen Mengingat bahwa bangsa terdiri atas elemen pemerintah, sektor swasta, komunitas akademik, dan masyarakat sipil, maka penguatan sistem pertahanan nasional memerlukan pendekatan kolaboratif lintas sektor. Untuk menjawab tantangan tersebut, penelitian ini merekomendasikan lima langkah strategis yang saling melengkapi. Pertama, diperlukan pelaksanaan reformasi birokrasi di lingkungan pertahanan guna menciptakan tata kelola yang transparan, akuntabel, dan responsif terhadap dinamika ancaman kontemporer. Kedua, peningkatan kapasitas sumber daya manusia menjadi prasyarat utama melalui pendidikan, pelatihan, serta rekrutmen berbasis kompetensi. Ketiga, pemanfaatan teknologi kecerdasan buatan dalam aktivitas operasional sehari-hari diharapkan dapat mempercepat proses pengambilan keputusan dan meningkatkan efisiensi sistem pertahanan. Keempat, transformasi budaya kerja harus dilakukan melalui pengurangan struktur hierarki yang berlebihan serta penerapan sistem merit dalam pembinaan karier aparatur pertahanan. Kelima, penguatan dukungan anggaran dan komitmen politik yang proporsional setara dengan negara-negara lain merupakan landasan keberlanjutan pembangunan pertahanan jangka panjang.

Abstract

This study discusses the urgency of enhancing the implementation of the Total People's Defense System (Pertahanan Rakyat Semesta) as an adaptive and strategic approach to strengthening Indonesia's national resilience amid increasingly complex and dynamic multidimensional threats. Contemporary threats to national security no longer stem solely from conventional military domains but also include cyberattacks, disinformation, pandemics, economic sabotage, and climate change. This research employs a qualitative descriptive method through literature review and analysis of national defense policies and international practices. The findings reveal that the implementation of the Total People's Defense System in Indonesia still faces several challenges, including weak cross-sectoral coordination, overlapping regulations, limited budget allocation, and low public defense literacy. The success of this system depends greatly on the active involvement of all national elements, including the government, private sector, academia, and civil society. To address these challenges, the study proposes five strategic recommendations: (1) implementing bureaucratic reform within the defense sector, (2) improving human resource capacity, (3) utilizing artificial intelligence (AI) technology in daily operations, (4) transforming rigid organizational culture by reducing excessive hierarchy and adopting a merit-based career system, and (5) ensuring political and budgetary support on par with other countries. Through these approaches, Indonesia can build a modern, inclusive, and adaptive defense system while strengthening national solidarity to safeguard stability and sovereignty.

Kata Kunci:

China Manuver;

Indo-Pacific;

Indonesia Defense;

Quad Policy;

Region Security.

Corresponding Author:

Faonaso Harefa,
Managemen Pertahanan
Universitas Pertahanan



PENDAHULUAN

Dalam era globalisasi yang semakin kompleks, keamanan nasional tidak lagi hanya bergantung pada kekuatan militer konvensional. Ancaman non-militer seperti “serangan siber, perubahan iklim, dan disinformasi menjadi tantangan baru yang harus dihadapi oleh negara-negara di seluruh dunia (Bergmann & Müller, 2021). Sebagai respons terhadap dinamika ini, konsep *Total Defense System* muncul sebagai model pertahanan yang lebih tangguh dan komprehensif (Larsson, 2021). *Total Defense System* adalah pendekatan yang melibatkan seluruh komponen masyarakat dalam membangun kesiapsiagaan nasional. Model ini pertama kali diterapkan di negara-negara seperti Swedia dan Singapura yang mengintegrasikan unsur militer dan sipil dalam strategi pertahanan (Ericson et al., 2023)”. Implementasi model ini terbukti efektif dalam menghadapi ancaman multidimensional dan dinamis seperti serangan siber (Wadjdi et al., 2024).

Implementasi Sistem Pertahanan dan keamanan rakyat Semesta (Sishankamrata) di Indonesia memiliki keselarasan dengan konsep *Total Defense System* tersebut. “Melalui pendekatan ini, negara harus meningkatkan ketahanan nasional dengan memberdayakan masyarakat sebagai bagian dari sistem pertahanan tersebut (Murfi et al., 2024). Walaupun demikian, masih terdapat berbagai tantangan dalam penerapan policy t ini, misalnya kurangnya koordinasi antar lembaga dan keterbatasan sumber daya manusia (Bergmann & Müller, 2021). Sebagai ancaman terbesar di era digital saat ini adalah serangan siber yang dapat menargetkan infrastruktur kritis, termasuk sistem keuangan, layanan kesehatan, dan sektor pemerintahan (Prakash et al., 2023). Ancaman non militer semakin nyata dan memiliki dampak luas terhadap ketahanan nasional, seperti serangan siber telah menjadi ancaman utama bagi infrastruktur kritis suatu negara, termasuk sistem pemerintahan, keuangan, serta sektor kesehatan (Prakash et al., 2023). Beberapa negara yang telah menerapkan strategi keamanan siber berbasis TDS terbukti lebih siap dalam menangani serangan ini secara efektif (Ericson et al., 2023). Sebagai contoh, Swedia telah mengembangkan strategi ketahanan digital yang melibatkan kolaborasi antara pemerintah dan perusahaan teknologi dalam menghadapi serangan siber (Rainey et al., 2021). Selain itu, pandemi Covid-19 menjadi bukti nyata bagaimana ancaman biologis dapat melemahkan perekonomian dan stabilitas sosial suatu negara. Negara-negara yang telah menerapkan model pertahanan total berbasis ketahanan kesehatan lebih mampu mengelola dampak pandemi secara efektif dibandingkan negara yang hanya mengandalkan respons darurat (Wrange, 2022). Sebagai perbandingan, Singapura berhasil menekan dampak pandemi dengan menerapkan sistem ketahanan kesehatan sebagai bagian dari strategi *Total Defence* mereka (Prakash et al., 2023). Ancaman disinformasi dan propaganda digital juga menjadi isu strategis dalam pertahanan nasional. Penyebaran hoaks dan manipulasi informasi melalui media sosial dapat melemahkan kohesi sosial serta mempengaruhi stabilitas politik suatu negara” (Bergmann & Müller, 2021).

Oleh karena itu, “strategi pertahanan negara harus meliputi program literasi digital dan penguatan sistem keamanan informasi guna menangkal ancaman propaganda by digital ini (Wadjdi et al., 2024). Walaupun Sistem Pertahanan Semesta telah diadopsi dalam kebijakan pertahanan Indonesia, implementasinya masih menghadapi berbagai kendala yang perlu segera diselesaikan: 1) Koordinasi antar-lembaga yang belum optimal. “Kebijakan pertahanan di Indonesia masih menghadapi fragmentasi antar kementerian seperti Kementerian Pertahanan, Badan Siber dan Sandi Negara (BSSN), serta BNPB, yang sering memiliki kebijakan tumpang tindih (Murfi et al., 2024), 2) Keterbatasan anggaran pertahanan”. Alokasi dana untuk pertahanan nasional masih cenderung lebih fokus pada penguatan kekuatan militer konvensional, sementara aspek ketahanan non-militer seperti keamanan siber dan kesiapsiagaan masyarakat, masih kurang mendapatkan perhatian (Bergmann & Müller, 2021), 3) Ancaman digital yang terus meningkat. Indonesia masih menghadapi kelemahan dalam sistem keamanan siber, dengan meningkatnya kasus peretasan terhadap infrastruktur digital pemerintahan dan sektor finansial (Ericson et al., 2023). Tanpa investasi yang memadai dalam teknologi pertahanan siber, Indonesia akan semakin rentan terhadap ancaman serangan digital (Prakash et al., 2023), 4) Kurangnya kesadaran masyarakat terhadap pertahanan nasional. Program edukasi terkait kesiapsiagaan nasional masih belum sepenuhnya terintegrasi dalam sistem pendidikan di Indonesia”. Banyak masyarakat yang

masih menganggap bahwa pertahanan negara hanyalah tanggung jawab militer, sehingga partisipasi publik dalam strategi pertahanan masih tergolong rendah (Wadjdi et al., 2024).

METODE

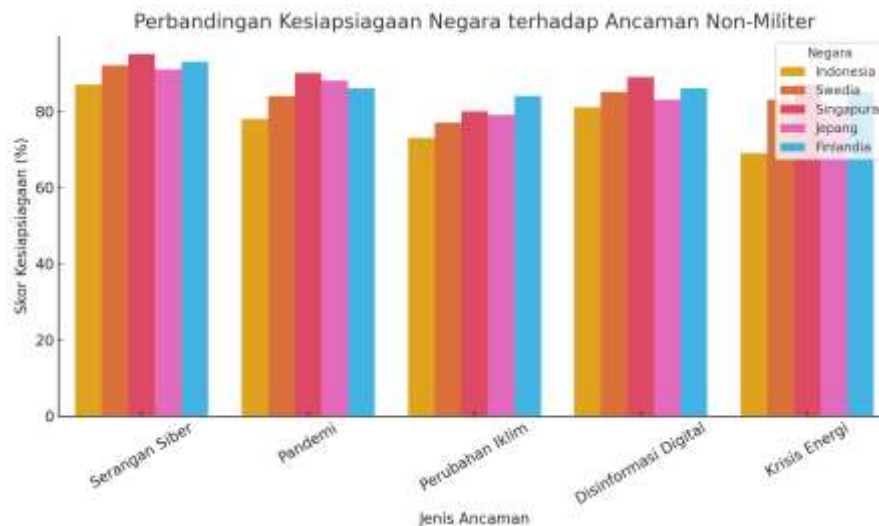
Penelitian ini menggunakan pendekatan kualitatif deskriptif untuk mengkaji secara mendalam implikasi kebijakan Pertahanan Negara dilihat dari “Kesiapsiagaan Sistem Pertahanan Total dalam Menghadapi Ancaman Non-Militer. Pendekatan ini dipilih karena mampu menangkap kompleksitas fenomena geopolitik yang multidimensional secara kontekstual, termasuk interaksi antar aktor negara dan non-negara dalam kerangka kepentingan nasional Indonesia. Teknik pengumpulan data dilakukan melalui analisis data sekunder artikel jurnal ilmiah, website dan dokumen terkait seperti undang-undang nomor 3 tahun 2002 tentang Pertahanan Negara, Undang-Undang no. 34 tahun 2004 tentang Tentara Nasional Indonesia, Kebijakan Umum Pertahanan negara periode 2025-2029, dan kebijakan penyelenggaraan pertahanan negara tahun 2025. Teknis analisis data dalam penelitian kualitatif deskriptif bertujuan untuk menggambarkan secara sistematis fenomena atau isu yang diteliti berdasarkan data yang dikumpulkan dari berbagai sumber. Proses ini diawali dengan tahap reduksi data, yaitu menyederhanakan, memilah, dan memfokuskan data yang relevan sesuai dengan fokus penelitian. Pada tahap ini, informasi yang tidak relevan dieliminasi, dan data yang ada kemudian dikelompokkan berdasarkan tema-tema tertentu seperti kebijakan, tantangan, aktor, dan strategi.” Untuk memastikan validitas, keterkinian, dan netralitas politik sumber data, penelitian ini menggunakan triangulasi sumber dengan mengutamakan dokumen dari dokumen negara dan jurnal terindeks scopus. Pemilihan data dibatasi pada periode setelah 2017, dengan fokus tematik Sistem pertahanan dan keamanan rakyat semesta (sishankamrata) Untuk membedakan opini dan fakta, peneliti menerapkan protokol validasi dengan melihat keberadaan bukti empiris, kredibilitas penulis atau institusi, serta kejelasan antara data objektif dan opini normatif. Artikel opini hanya digunakan jika relevan secara kontekstual dan dianalisis secara kritis.

PEMBAHASAN

Perubahan dalam melihat keamanan global telah memaksa negara-negara untuk mengadopsi pendekatan pertahanan yang lebih inklusif dan terintegrasi, salah satunya melalui *Total Defense System*. “Model pertahanan ini mengedepankan keterlibatan seluruh elemen masyarakat dalam upaya mempertahankan keamanan nasional secara menyeluruh (Larsson, 2021). “Konsep *Total Defense System* bukanlah pendekatan baru dalam kebijakan pertahanan negara. Sejak Perang Dingin, beberapa negara telah menerapkan sistem ini untuk membangun ketahanan nasional yang lebih komprehensif (Ericson et al., 2023)”. Indonesia telah mengadopsi model yang serupa dalam bentuk Sistem Pertahanan Semesta (Sishanta), yang melibatkan keterlibatan semua komponen bangsa dalam sistem pertahanan nasional (Murfi et al., 2024). Namun, pelaksanaan kebijakan ini masih menghadapi berbagai tantangan, termasuk fragmentasi kebijakan antar lembaga, keterbatasan anggaran, serta rendahnya partisipasi masyarakat dalam kesiapsiagaan nasional (Bergmann & Müller, 2021). Untuk mencapai efektivitas yang lebih tinggi, implementasi *Total Defense System* di Indonesia perlu disesuaikan dengan konteks sosial, ekonomi, dan geopolitik yang lebih luas”. *Total Defense System* memainkan peran penting dalam memperkuat stabilitas dan ketahanan nasional. Dengan melibatkan seluruh sektor masyarakat, TDS tidak hanya berfungsi dalam menghadapi ancaman militer, tetapi juga mengatasi krisis nasional yang dapat berdampak luas pada aspek ekonomi, sosial, dan politik (Prakash et al., 2023). Beberapa kontribusi utama dari implementasi TDS dalam kebijakan pertahanan nasional meliputi: “1) Meningkatkan kesiapsiagaan nasional terhadap ancaman multidimensi. Pendekatan ini memungkinkan negara untuk memiliki resiliensi yang lebih tinggi dalam menghadapi ancaman non-militer seperti bencana alam, krisis energi, dan pandemi (Larsson, 2021), 2) Memperkuat kolaborasi antara pemerintah dan masyarakat. Sinergi antara lembaga negara, sektor swasta, akademisi, dan masyarakat sipil mempercepat respons dalam situasi darurat (Ericson et al., 2023), 3) Mengurangi ketergantungan pada kekuatan militer konvensional. Dengan melibatkan sektor non-militer, negara dapat mengoptimalkan sumber daya yang lebih luas dalam mempertahankan stabilitas nasional (Bergmann & Müller, 2021), 4) Meminimalisir dampak serangan siber dan disinformasi. Peningkatan literasi digital dan perlindungan terhadap infrastruktur digital nasional menjadi aspek penting dalam TDS (Wadjdi et al., 2024). Implementasi *Total Defense System* di Indonesia tidak hanya relevan untuk menghadapi ancaman eksternal, tetapi juga sebagai strategi mitigasi risiko dalam skala nasional”.

Penguatan *Total Defense System* dalam menghadapi ancaman kontemporer di era modern, “ancaman non-militer tidak hanya berasal dari serangan fisik, tetapi juga mencakup dimensi yang lebih luas seperti ancaman ekonomi, serangan biologis, dan disrupsi sosial akibat propaganda digital. Globalisasi telah menyebabkan negara-negara semakin saling terhubung, yang berarti bahwa sebuah ancaman di satu negara dapat berdampak signifikan terhadap negara lain. Beberapa negara maju telah memasukkan adaptasi perubahan iklim sebagai bagian dari strategi pertahanan mereka dan Indonesia perlu mengadopsi langkah serupa untuk memastikan keberlanjutan kebijakan pertahanan nasional dalam jangka panjang (Larsson, 2021). Penerapan *Total Defense System* yang efektif memiliki dampak luas terhadap berbagai aspek ketahanan nasional, diantaranya: 1) Ketahanan Ekonomi. Dengan adanya integrasi antara sektor pertahanan dan ekonomi, suatu negara dapat lebih siap menghadapi disrupsi global yang disebabkan oleh krisis keuangan, embargo ekonomi, atau gangguan dalam rantai pasokan global, 2) Ketahanan Sosial. Peningkatan literasi pertahanan di masyarakat melalui pendidikan dan pelatihan akan membangun kesadaran nasional yang lebih tinggi serta meningkatkan partisipasi masyarakat dalam sistem pertahanan negara, 3) Ketahanan Teknologi dan Siber. Negara yang memiliki strategi pertahanan siber yang kuat akan lebih mampu menangkal ancaman siber yang berkembang pesat serta menghindari dampak besar akibat kebocoran data nasional, 4) Ketahanan Politik. Kestabilan politik dalam negeri dapat terjaga dengan baik jika pemerintah memiliki sistem pertahanan yang solid dalam menghadapi propaganda asing, infiltrasi ideologi radikal, serta ancaman terhadap keamanan nasional. Dengan kata lain, keberhasilan implementasi *Total Defense System* di Indonesia tidak hanya berdampak pada aspek militer tetapi juga berkontribusi terhadap kesejahteraan dan keamanan masyarakat secara keseluruhan”.

Negara-negara dengan sistem pertahanan yang kuat telah menerapkan konsep *Total Defense System* dengan pendekatan yang berbeda, berikut dua contoh negara yang berhasil menerapkan TDS dalam kebijakan nasional mereka: “1) Swedia menerapkan strategi *total försvaret* yang mencakup koordinasi antara sektor pertahanan militer, keamanan siber, dan kesiapsiagaan masyarakat. Negara ini memiliki kebijakan ketahanan pangan dan energi yang terintegrasi dalam strategi pertahanan nasional yang memungkinkan mereka untuk tetap mandiri dalam situasi krisis global, 2) Singapura dengan Model Total Defence. Singapura mengembangkan model Total Defence, sebuah strategi pertahanan komprehensif yang mengintegrasikan enam pilar utama, yaitu pertahanan militer, pertahanan sipil, ketahanan ekonomi, ketahanan sosial, ketahanan psikologis, dan keamanan digital”. Model ini dirancang untuk memastikan kesiapsiagaan nasional terhadap berbagai ancaman modern, termasuk serangan militer, bencana alam, krisis ekonomi, serta ancaman berbasis teknologi seperti serangan siber dan disinformasi.



Gambar 1. Perbandingan Kesiapsiagaan Negara terhadap Ancaman Non-Militer

Cybersecurity Index (2021), Munich Security Index (2024), dan WorldRiskIndex (2021). “Data tersebut menunjukkan bahwa negara-negara seperti Singapura, Finlandia, dan Swedia memiliki skor kesiapsiagaan yang tinggi, rata-rata di atas 85% dalam menghadapi ancaman digital dan krisis biologis. Sebaliknya, Indonesia menunjukkan kesenjangan signifikan, khususnya dalam kesiapsiagaan terhadap

krisis energi dan perubahan iklim, dengan skor di bawah 75%. Hal ini menegaskan bahwa Indonesia masih berada dalam tahap awal dalam membangun sistem ketahanan menyeluruh yang berbasis pada *Total Defense System* (TDS). Skor kesiapsiagaan yang lebih tinggi di negara-negara tersebut tidak terlepas dari penerapan sistem pertahanan total yang melibatkan koordinasi lintas sektor, investasi pada keamanan digital, serta integrasi pelatihan sipil dalam sistem pendidikan nasional (Ericson et al., 2023; Wang & Xu, 2022). Sebaliknya, di Indonesia, pendekatan kebijakan yang masih terfragmentasi dan terbatasnya alokasi anggaran pada sektor non-militer menjadi faktor utama penghambat pembangunan ketahanan nasional yang adaptif”.

Konsep Dasar *Total Defense System*.

Total Defense System (TDS) “merupakan konsep strategis dalam pertahanan nasional modern yang menekankan keterlibatan seluruh komponen bangsa dalam menghadapi berbagai bentuk ancaman, baik militer maupun non-militer. Pendekatan ini berpijak pada asumsi bahwa pertahanan negara tidak dapat hanya disandarkan pada kekuatan militer konvensional semata, tetapi memerlukan partisipasi aktif dari pemerintah, sektor swasta, masyarakat sipil, dunia pendidikan, serta komunitas lokal (Bergmann & Müller, 2021). Secara teoritik, konsep TDS berakar pada pendekatan *comprehensive security* dan *human security*, di mana keamanan tidak hanya diartikan sebagai perlindungan dari agresi eksternal, tetapi juga mencakup dimensi sosial, ekonomi, lingkungan, dan teknologi yang memengaruhi stabilitas suatu negara (Buzan et al., 1998; Kivimaa et al., 2020). Dalam konteks ini, negara berfungsi sebagai fasilitator dan koordinator dari upaya kolektif seluruh elemen bangsa dalam membangun ketahanan nasional yang menyeluruh dan berlapis. TDS mencakup beberapa pilar utama yang terintegrasi dalam kebijakan pertahanan nasional: Pertahanan Militer, merupakan komponen kunci dalam menghadapi ancaman konvensional dan non-konvensional. Fokusnya meliputi modernisasi alutsista, peningkatan kapasitas personel militer, dan penguatan komando terpadu dalam situasi krisis. Pendekatan ini mengacu pada teori deterensi dan supremasi strategis dalam studi keamanan (Prakash et al., 2023). Pertahanan Sipil, yang menitikberatkan pada penguatan kapasitas masyarakat dan institusi sipil dalam menghadapi bencana alam, ancaman biologis, serta serangan siber. Hal ini mencakup sistem tanggap darurat, pelatihan publik, pengelolaan logistik, serta simulasi evakuasi terpadu (Ericson & Wester, 2022). Pilar ini menegaskan pentingnya resilien sosial sebagai benteng pertama dalam menghadapi disrupsi non-militer. Ketahanan Ekonomi, yang berfokus pada kemandirian produksi nasional, keberlanjutan logistik, dan daya tahan industri pertahanan. Di saat krisis global atau embargo ekonomi, kemampuan negara untuk memenuhi kebutuhan dasar dan mempertahankan stabilitas ekonomi menjadi faktor vital (Wrange et al., 2024; Nesvetailova & Palan, 2021). Pilar ini erat kaitannya dengan teori ekonomi pertahanan dan strategi *supply chain* nasional. Ketahanan Sosial dan Psikologis, yang bertujuan menjaga kohesi sosial, memperkuat identitas nasional, serta meningkatkan resiliensi masyarakat terhadap disinformasi, ujaran kebencian, dan propaganda asing”. Dalam TDS, ketahanan psikososial dipandang sebagai lapisan pertahanan yang menjaga keutuhan bangsa dari fragmentasi sosial (Boin et al., 2022). “Keamanan Digital dan Siber, sebagai respons terhadap meningkatnya intensitas ancaman digital terhadap sistem pemerintahan, infrastruktur publik, dan data strategis. Pilar ini menekankan pentingnya regulasi keamanan siber nasional, pembangunan kapasitas cyber intelligence, serta partisipasi sektor teknologi dalam memperkuat ekosistem pertahanan digital (Wang & Xu, 2022; Chertoff & Simon, 2021)”. TDS bukanlah pendekatan yang statis, melainkan dinamis dan adaptif terhadap evolusi ancaman global. Dalam praktiknya, keberhasilan penerapan TDS sangat bergantung pada sinergi antarpilar, perencanaan lintas sektor yang matang, serta partisipasi aktif dari masyarakat. Oleh karena itu, integrasi TDS dalam arsitektur pertahanan negara memerlukan kebijakan yang bersifat holistik, multisektor, dan inklusif untuk menjamin ketahanan nasional yang berkelanjutan.

Implementasi *Total Defense System* di negara lain.

Implementasi *Total Defense System* (TDS) telah diterapkan dengan beragam pendekatan di berbagai negara, menyesuaikan dengan karakteristik geopolitik, sosial, dan kapasitas institusional masing-masing. “Negara-negara yang sukses mengimplementasikan TDS umumnya menempatkan kerja sama antara komponen militer dan sipil sebagai pilar utama dalam menjaga ketahanan nasional. Keberhasilan mereka dapat menjadi referensi penting bagi Indonesia dalam membangun sistem TDS yang efektif dan adaptif terhadap ancaman kontemporer. Swedia merupakan contoh paling menonjol dalam penerapan *Totalförsvaret*, yaitu model pertahanan total yang mengintegrasikan pemerintah pusat, daerah, sektor swasta, dan masyarakat sipil dalam satu sistem koordinatif. Swedia telah mengembangkan struktur komando gabungan dan sistem logistik yang mencakup persiapan bencana

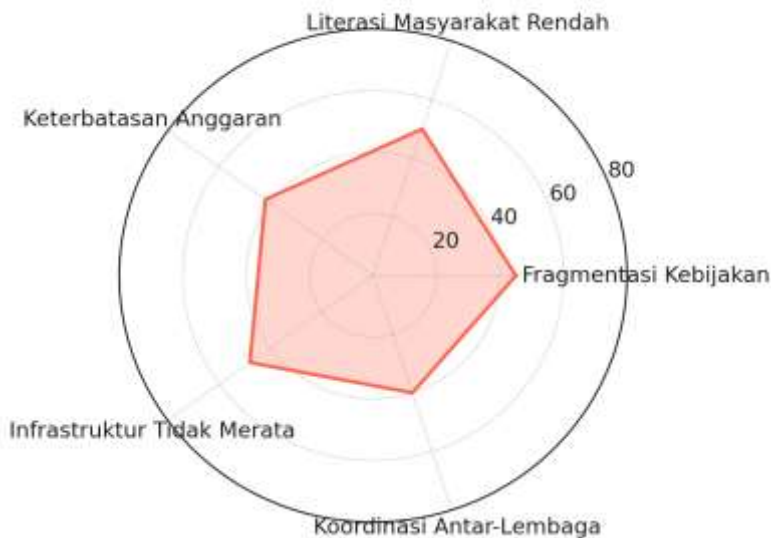
alam, serangan siber, serta konflik bersenjata”. “Pusat-pusat pelatihan sipil disediakan oleh pemerintah untuk masyarakat umum, termasuk program simulasi tanggap darurat dan peran sipil dalam masa krisis (Ericson et al., 2023; Wrange et al., 2024). Singapura mengembangkan *Total Defence Strategy* sejak 1984 dan menyempurnakannya hingga mencakup enam pilar utama: pertahanan militer, sipil, ekonomi, sosial, psikologis, dan digital. Model ini mendorong partisipasi aktif seluruh lapisan masyarakat, mulai dari institusi pendidikan, industri teknologi, media massa, hingga organisasi kemasyarakatan. Strategi ini juga didukung oleh kampanye nasional tahunan dan integrasi kurikulum pendidikan bela negara sejak tingkat dasar hingga universitas (Raska & Bitzinger, 2022). Pusat Keamanan Siber Nasional di Singapura menjadi bukti nyata integrasi pilar digital dalam pertahanan semesta. Jepang menempatkan konsep *Comprehensive National Security Strategy* sebagai acuan utama dalam merespons ancaman multidimensi. Strategi ini menggabungkan elemen diplomasi, militer, ekonomi, dan siber dalam kebijakan luar negeri dan dalam negeri. Jepang aktif mengembangkan sistem peringatan dini, memperkuat jaringan keamanan energi, serta menginvestasikan dana besar dalam pengembangan teknologi pertahanan otonom, seperti sistem satelit pemantau dan kendaraan udara nirawak (Ericson et al., 2023; Wang & Xu, 2022). Sementara itu, Finlandia mengadopsi pendekatan *Comprehensive Security Model* yang menempatkan ketahanan nasional sebagai hasil kerja sama antara lembaga pemerintahan, sektor swasta, komunitas lokal, dan universitas. Model ini memiliki keunikan dalam pengelolaan latihan nasional berskala besar yang melibatkan warga sipil secara aktif, serta integrasi manajemen krisis lingkungan sebagai bagian dari sistem pertahanan (Kivimaa et al., 2020). Pemerintah Finlandia juga menyusun skenario ancaman nasional secara berkala untuk memperkuat kapasitas antisipatif dalam sistem perencanaan pertahanannya”. “Pengalaman keempat negara tersebut menunjukkan bahwa keberhasilan TDS sangat ditentukan oleh tiga hal utama: sinergi antar pemangku kepentingan, kejelasan pembagian peran, dan investasi dalam pendidikan serta teknologi. Model seperti Swedia dan Finlandia menonjol dalam aspek kesiapsiagaan sipil dan lingkungan, sementara Singapura dan Jepang unggul dalam pengembangan sistem teknologi pertahanan dan koordinasi digital”. Kombinasi dari praktik-praktik terbaik ini dapat dijadikan rujukan dalam merumuskan arsitektur pertahanan semesta Indonesia yang adaptif, progresif, dan berkelanjutan.

Tantangan Implementasi di Indonesia.

Indonesia menghadapi beberapa tantangan besar dalam mengimplementasikan *Total Defence System* (TDS) secara menyeluruh. Salah satu hambatan utama adalah; “fragmentasi kebijakan antar-lembaga yang menyebabkan tumpang tindih fungsi dan ketidakefisienan dalam pelaksanaan program. Kementerian Pertahanan, Badan Siber dan Sandi Negara (BSSN), Badan Nasional Penanggulangan Bencana (BNPB), dan instansi lainnya sering kali bekerja secara terpisah tanpa koordinasi terpadu, sehingga menghambat respons nasional yang terintegrasi (Murfi et al., 2024). Tantangan lainnya adalah rendahnya literasi digital dan kesadaran pertahanan di kalangan masyarakat, yang berdampak pada kurangnya partisipasi publik dalam mendukung kebijakan pertahanan non-militer. Sebuah survei oleh Wadjdi et al. (2024) menunjukkan bahwa sebagian besar masyarakat Indonesia masih menganggap bahwa pertahanan hanya tugas militer, dan belum memahami peran aktif mereka dalam konteks ancaman non-tradisional seperti disinformasi atau serangan siber”.

Anggaran juga menjadi kendala besar, “terutama dalam alokasi untuk sektor-sektor non-militer seperti kesiapsiagaan sipil, teknologi keamanan siber, dan edukasi pertahanan. Mayoritas anggaran pertahanan masih terserap untuk belanja alutsista dan infrastruktur militer, sementara pengembangan sistem peringatan dini, program pelatihan masyarakat, dan digitalisasi sistem pertahanan nasional belum menjadi prioritas (Larsson, 2021). Selain itu, infrastruktur pendukung untuk TDS, seperti sistem logistik darurat, komunikasi lintas sektor, serta fasilitas pelatihan terpadu bagi sipil dan militer, belum berkembang secara optimal. Banyak daerah, khususnya di wilayah timur Indonesia, masih menghadapi keterbatasan dalam akses logistik dan teknologi dasar, yang membuat pemerataan kesiapsiagaan menjadi tantangan tersendiri (Kavakli & Zhu, 2023). Ketimpangan geografis, keberagaman sosial budaya, serta resistensi terhadap perubahan kebijakan juga memperkuat kompleksitas tantangan implementasi TDS. Oleh karena itu, diperlukan pendekatan kebijakan yang adaptif, inklusif, dan berbasis data untuk memastikan bahwa seluruh komponen bangsa dapat berperan aktif dalam sistem pertahanan nasional yang tangguh dan berkelanjutan”.

Tantangan Implementasi TDS di Indonesia



Gambar 2. Tantangan Implementasi TDS di Indonesia

Gambar ini memperlihatkan lima tantangan utama dalam implementasi *Total Defense System* di Indonesia yaitu “Nilai kesiapan pada setiap dimensi menunjukkan bahwa tantangan paling signifikan terletak pada koordinasi antar-lembaga” (skor 40) dan keterbatasan anggaran untuk sektor non-militer (skor 42). Selain itu, fragmentasi kebijakan (45) dan infrastruktur yang tidak merata (48) menghambat integrasi lintas sektor dan efektivitas kebijakan TDS di tingkat nasional dan daerah. Literasi masyarakat yang rendah terhadap peran sipil dalam pertahanan (skor 50) juga menjadi hambatan partisipatif yang krusial. Data ini disusun berdasarkan analisis dari *Global Health Security Index* (GHSI), *Global Cybersecurity Index* (GCI), serta laporan *Munich Security Index* dan *WorldRiskIndex*, yang menempatkan Indonesia dalam kategori kesiapsiagaan sedang hingga rendah untuk berbagai indikator non-militer. Upaya pembangunan TDS di Indonesia harus difokuskan pada penguatan koordinasi kelembagaan, peningkatan kapasitas masyarakat, dan alokasi anggaran yang lebih proporsional untuk mendukung pertahanan non-tradisional secara menyeluruh”.

Strategi Penguatan *Total Defense System* di Indonesia.

Untuk memperkuat *Total Defense System*, Indonesia perlu mengadopsi strategi yang bersifat lintas sektor dan terintegrasi. “1) pembentukan lembaga koordinatif nasional yang secara khusus menangani perencanaan dan pengawasan pelaksanaan TDS sangat krusial. Lembaga ini harus memiliki otoritas lintas kementerian untuk menghindari fragmentasi kebijakan dan memperkuat koordinasi antar aktor negara; 2) penguatan kerangka hukum dan peraturan pendukung sangat penting untuk memperjelas peran serta tanggung jawab masing-masing lembaga, baik di tingkat pusat maupun daerah. Regulasi ini harus mencakup kewajiban pelatihan kesiapsiagaan bagi warga negara, integrasi program TDS dalam RPJMN, serta mekanisme pembiayaan yang transparan; 3) investasi dalam infrastruktur teknologi dan keamanan siber harus diprioritaskan untuk mendukung perlindungan data strategis dan sistem pemerintahan digital. Pemerintah perlu menggandeng sektor swasta dan akademisi dalam membangun pusat inovasi keamanan nasional yang berfokus pada pengembangan AI, analisis big data, dan simulasi krisis (Wadjdi et al., 2024). 4) penguatan literasi pertahanan dan kesiapsiagaan nasional melalui pendidikan formal dan informal. Integrasi materi pertahanan semesta ke dalam kurikulum pendidikan dasar hingga perguruan tinggi harus disertai pelatihan praktis seperti latihan evakuasi, simulasi krisis, dan pengenalan teknologi digital pertahanan. Program bela negara berbasis komunitas juga perlu digalakkan untuk memperluas partisipasi masyarakat; 5) diplomasi pertahanan harus diintensifkan, terutama dengan negara-negara yang telah sukses mengimplementasikan TDS. Kerja sama strategis dalam bentuk pertukaran teknologi, pelatihan bersama, dan pembentukan forum regional terkait ketahanan non-militer akan memperkuat kapabilitas nasional. Dengan menerapkan strategi-strategi tersebut, Indonesia akan memiliki sistem pertahanan nasional yang tidak hanya

tangguh menghadapi ancaman militer konvensional, tetapi juga responsif dan adaptif terhadap dinamika ancaman non-militer yang terus berkembang”.

Peran Pemerintah dalam mengoptimalkan *Total Defense System*.

Pemerintah memiliki peran sentral dalam mengimplementasikan TDS secara efektif di Indonesia. Pemerintah bertugas merumuskan regulasi, menetapkan anggaran, dan mengkoordinasikan pelaksanaan TDS. “Pembentukan Badan Koordinasi Pertahanan Non-Militer Nasional dapat menjadi solusi untuk menghindari tumpang tindih fungsi. Lembaga seperti BSSN dan BNPB harus diberdayakan sebagai garda depan pertahanan non-militer. Kebijakan ini juga harus memperkuat partisipasi masyarakat sipil dan akademisi (Jensen, 2021). Langkah-langkah yang dapat diambil oleh pemerintah antara lain: 1) Meningkatkan kebijakan perlindungan infrastruktur digital nasional guna menghadapi serangan siber yang semakin kompleks, 2) Memperkuat koordinasi antara sektor militer dan sipil untuk menciptakan sistem pertahanan yang lebih terintegrasi (Murfi et al., 2024), 3) Menyusun regulasi tentang keterlibatan sektor swasta dalam sistem pertahanan nasional agar industri dapat berkontribusi dalam penguatan ekonomi pertahanan. Globalisasi telah membawa perubahan dalam cara suatu negara merancang sistem pertahanannya”. Dengan meningkatnya keterhubungan antarnegara, ancaman yang dihadapi tidak lagi bersifat tradisional melainkan lebih kompleks dan multidimensional (Bergmann & Müller, 2021).

Peran strategis generasi muda dan pendidikan bela negara.

Keterlibatan generasi muda merupakan fondasi utama dalam menjamin keberlangsungan dan efektivitas jangka panjang dari *Total Defense System*. “Dalam konteks demografi Indonesia yang didominasi oleh penduduk usia muda, potensi ini harus dioptimalkan melalui kebijakan pendidikan, pelatihan, dan pemberdayaan berbasis bela negara. Pendidikan bela negara tidak hanya harus menjadi bagian dari narasi formal, tetapi juga terintegrasi secara fungsional dan aplikatif ke dalam kurikulum pendidikan dasar hingga perguruan tinggi. Materi pendidikan bela negara harus diperluas untuk mencakup isu-isu kontemporer seperti keamanan siber, literasi digital, manajemen risiko, mitigasi bencana, komunikasi krisis, dan pemulihan pasca-bencana. Metode pengajaran pun perlu disesuaikan dengan karakteristik generasi digital, dengan pendekatan berbasis simulasi, studi kasus, permainan strategi, dan teknologi digital (Setyawan & Rahardjo, 2022). Upaya ini bertujuan menciptakan pemahaman mendalam dan rasa tanggung jawab terhadap pertahanan negara di kalangan pemuda”.

Pemerintah dapat menginisiasi program seperti *Youth National Resilience Corps*, sebuah unit cadangan berbasis kampus yang menggabungkan unsur pelatihan fisik, intelektual, dan digital dalam membangun kapasitas pertahanan generasi muda. Program serupa telah sukses diterapkan di Taiwan dan Israel, yang menempatkan pemuda sebagai aktor strategis dalam kesiapsiagaan nasional serta pilar utama dalam sistem pertahanan populasi (Ahronheim, 2022; Barnea & Harel, 2021).”Selain pendidikan formal, penguatan bela negara juga dapat dilakukan melalui organisasi kemasyarakatan, pelatihan berbasis komunitas, serta platform digital berbasis edukasi. Misalnya, platform seperti aplikasi *e-bela negara* dapat dikembangkan sebagai media pembelajaran interaktif dan alat monitoring partisipasi warga negara dalam latihan kesiapsiagaan. Peran universitas juga krusial sebagai pusat kajian strategis dan laboratorium kebijakan pertahanan semesta (Boin et al., 2022). Lebih jauh, keterlibatan generasi muda tidak boleh bersifat simbolik. Pemuda harus diberi ruang aktualisasi dalam penyusunan kebijakan pertahanan, pengembangan teknologi keamanan, serta keterlibatan dalam forum internasional terkait keamanan dan diplomasi pertahanan. Hal ini akan membangun generasi yang tidak hanya sadar ancaman, tetapi juga mampu menjadi agen perubahan dan pemimpin di sektor pertahanan nasional masa depan. Dengan demikian, investasi dalam pendidikan bela negara dan pemberdayaan pemuda merupakan langkah strategis untuk menciptakan sistem pertahanan nasional yang adaptif, inklusif, dan berkelanjutan”.

Strategi Digital dan Perang Informasi dalam TDS

Ancaman digital seperti; “disinformasi, propaganda, dan serangan siber memerlukan respons terstruktur. Strategi TDS harus mencakup deteksi hoaks berbasis AI, edukasi literasi digital massal, dan pembangunan *cyber reserve corps*. “Kerja sama internasional dalam pertahanan siber melalui ASEAN *Cyber Security Cooperation* juga perlu ditingkatkan (Gillespie & O’Loughlin, 2020; Chertoff & Simon, 2021). Perang informasi merupakan ancaman kontemporer yang melibatkan manipulasi data, propaganda, dan penyebaran hoaks yang sistematis. Studi oleh Gillespie & O’Loughlin (2020) menjelaskan bahwa perang informasi bertujuan melemahkan legitimasi pemerintah dan membelah

masyarakat. Dalam konteks Indonesia, pemilu, isu agama, dan konflik identitas sering kali menjadi sasaran utama operasi disinformasi. Untuk menghadapinya, strategi digital dalam TDS harus mencakup tiga aspek: (1) infrastruktur siber yang kuat, (2) sistem deteksi hoaks berbasis AI, dan (3) literasi digital masyarakat. Pemerintah juga dapat mengembangkan *cyber reserve corps* yang melibatkan pemuda terlatih sebagai pasukan pertahanan digital nasional (Chertoff & Simon, 2021)". Kerja sama internasional dalam pertahanan siber pun perlu diperkuat, termasuk melalui *ASEAN Cybersecurity Cooperation Strategy*.

Dimensi Ketahanan Non-Militer (Ekonomi, Sosial, Teknologi, dan Lingkungan)

Ketahanan ekonomi diperkuat melalui; "diversifikasi sumber daya dan proteksi sektor kritis (Kavakli & Zhu, 2023; Nesvetailova & Palan, 2021). "Ketahanan sosial terbentuk dari partisipasi publik dan kepercayaan pada institusi (Boin et al., 2022). Teknologi digital, seperti AI dan IoT, memperkuat deteksi dini dan respons krisis (Wang & Xu, 2022). Ketahanan lingkungan melalui mitigasi perubahan iklim dan penguatan kesiapsiagaan bencana harus menjadi bagian dari kebijakan pertahanan nasional (Kivimaa et al., 2020). Penerapan TDS yang efektif tidak hanya bergantung pada kesiapan militer dan sipil, tetapi juga pada ketahanan ekonomi dan sosial. Ketahanan ekonomi dalam konteks TDS mengacu pada kemampuan suatu negara untuk mempertahankan kestabilan produksi, distribusi, dan konsumsi nasional dalam menghadapi krisis (Kavakli & Zhu, 2023). Negara-negara yang memiliki cadangan pangan strategis, diversifikasi energi, dan proteksi terhadap industri kritikal cenderung lebih mampu menghadapi embargo ekonomi atau guncangan pasokan global (Nesvetailova & Palan, 2021). Ketahanan sosial berkaitan erat dengan kohesi sosial, kepercayaan publik terhadap negara, dan literasi informasi. Sebuah studi oleh Boin et al. (2022)", menunjukkan bahwa negara dengan tingkat kepercayaan publik tinggi dan partisipasi masyarakat yang kuat memiliki kapasitas respons krisis yang lebih baik. Ini menjadi sangat relevan di tengah ancaman disinformasi dan manipulasi psikologis dalam perang hibrida.

Dalam era Revolusi Industri 4.0, dimensi teknologi juga menjadi aspek vital. Negara yang mengintegrasikan "teknologi kecerdasan buatan (AI), analisis big data, dan *Internet of Things* (IoT) dalam strategi TDS lebih cepat dalam mendeteksi dan merespons ancaman (Wang & Xu, 2022). Hal ini terlihat dari negara-negara seperti Korea Selatan dan Estonia yang berhasil membangun infrastruktur digital pertahanan nasional untuk melawan ancaman siber. Sementara itu, ketahanan lingkungan menjadi dimensi baru dalam pertahanan non-militer. Perubahan iklim, bencana alam, dan degradasi lingkungan kini masuk dalam indikator risiko strategis global. Negara seperti Jepang dan Finlandia telah memasukkan manajemen lingkungan ke dalam strategi pertahanan komprehensif mereka (Kivimaa et al., 2020). Indonesia perlu segera mengintegrasikan mitigasi risiko lingkungan ke dalam sistem TDS nasional.

Diplomasi Pertahanan dan Aliansi Strategis

Dalam kerangka *Total Defense System* (TDS), "diplomasi pertahanan menjadi elemen strategis yang tidak dapat dipisahkan dari upaya pembangunan ketahanan nasional yang menyeluruh. Diplomasi pertahanan bukan hanya bertujuan untuk membangun kepercayaan dan mencegah konflik antarnegara, tetapi juga untuk memperkuat kerja sama lintas sektor dalam menghadapi ancaman non-militer yang bersifat transnasional, seperti siber, disinformasi, krisis energi, dan bencana iklim (Raska & Bitzinger, 2022). Indonesia perlu memperluas jaringan aliansi pertahanan melalui kerja sama bilateral dan multilateral, terutama dengan negara-negara yang telah sukses menerapkan pendekatan TDS seperti Finlandia, Jepang, dan Singapura. Bentuk kerja sama yang perlu ditingkatkan antara lain: pertukaran teknologi strategis, pelatihan bersama dalam penanggulangan bencana dan keamanan siber, serta kolaborasi dalam pengembangan sistem *early warning regional* (Wong et al., 2023). Keikutsertaan aktif Indonesia dalam forum seperti *ASEAN Defence Ministers' Meeting-Plus* (ADMM-Plus), ASEAN Regional Forum (ARF), serta kerja sama trilateral Indonesia-Malaysia-Filipina di kawasan Laut Sulu-Sulawesi menunjukkan pentingnya peran regional dalam mendukung ketahanan nasional berbasis TDS". Forum-forum ini juga berfungsi sebagai arena untuk memperkuat interoperabilitas antara aparat sipil dan militer dari negara-negara mitra (Acharya, 2023).

Di tingkat global, "kontribusi Indonesia dalam misi pemeliharaan perdamaian PBB (UNPKO) merupakan instrumen diplomasi pertahanan yang efektif dalam menunjukkan komitmen terhadap keamanan kolektif serta memperkuat kompetensi pasukan Indonesia dalam menghadapi krisis multidimensi. Keterlibatan ini juga meningkatkan reputasi Indonesia sebagai kekuatan pertahanan berbasis semesta yang aktif di ranah internasional (UN Peacekeeping, 2022). Untuk memperkuat

dimensi teknologi dalam TDS, Indonesia dapat membangun kemitraan riset dan pengembangan bersama negara-negara yang memiliki keunggulan dalam bidang pertahanan digital, kecerdasan buatan (AI), dan keamanan maritim. Kemitraan ini tidak hanya akan memperkuat kapabilitas pertahanan nasional, tetapi juga mengurangi ketergantungan pada produk luar negeri dan meningkatkan kemandirian sistem pertahanan. Dengan pendekatan diplomasi pertahanan yang terencana, kolaboratif, dan berorientasi masa depan, Indonesia dapat memperkuat posisi sebagai stabilisator regional dan sekaligus memperluas jejaring dukungan global dalam menghadapi tantangan pertahanan abad ke-21. “Grafik jaringan ini menggambarkan posisi strategis Indonesia dalam menjalin kerja sama pertahanan dengan berbagai aktor internasional. Indonesia berada di pusat jejaring, terhubung dengan mitra utama seperti Singapura, Jepang, Amerika Serikat, Australia, dan negara-negara Eropa seperti Finlandia dan Swedia, yang dikenal sebagai pelaksana TDS yang efektif. Hubungan kelembagaan juga diperkuat melalui forum regional dan global seperti ASEAN dan *United Nations Peacekeeping Operations* (UNPKO). Jaringan ini menunjukkan bahwa keberhasilan TDS tidak dapat dilepaskan dari diplomasi pertahanan yang proaktif, pertukaran teknologi, pelatihan bersama, dan aliansi kebijakan keamanan siber serta krisis global”.

Evaluasi Kesiapan Nasional dan Rekomendasi Implementatif

Agar implementasi *Total Defense System* (TDS) berjalan efektif dan berkelanjutan, diperlukan evaluasi yang sistematis, berbasis data, dan menyeluruh. “Evaluasi ini harus mencakup indikator kuantitatif dan kualitatif yang merepresentasikan kesiapan nasional dalam menghadapi ancaman multidimensi. Indikator utama meliputi: (1) tingkat koordinasi lintas sektor dan antarlembaga pemerintah, (2) kesiapan dan keamanan infrastruktur digital, (3) indeks kesiapsiagaan dan partisipasi masyarakat, (4) proporsi anggaran pertahanan untuk sektor non-militer, serta (5) tingkat keterlibatan sektor pendidikan, swasta, dan komunitas dalam ekosistem TDS (Ericson et al., 2023; Boin et al., 2022). Koordinasi antar lembaga dapat diukur melalui kehadiran regulasi yang harmonis, frekuensi pertemuan lintas institusi, dan efektivitas pelaksanaan protokol manajemen krisis nasional. Dalam konteks digital, kesiapan dapat ditinjau melalui keberadaan pusat data nasional, sistem perlindungan siber, serta tingkat penggunaan teknologi AI dan big data dalam sistem peringatan dini (Wang & Xu, 2022). Partisipasi masyarakat diukur dari keterlibatan dalam pelatihan bela negara, keikutsertaan dalam simulasi bencana, serta hasil survei indeks kesadaran pertahanan. Alokasi anggaran juga menjadi instrumen krusial evaluasi”. Proporsi anggaran yang terlalu berat ke sektor militer konvensional tanpa memperhatikan aspek sipil dan sosial menunjukkan kurangnya keseimbangan dalam pendekatan TDS. Negara-negara seperti Swedia dan Singapura mengalokasikan sekitar 30-40% dari anggaran pertahanan mereka untuk program kesiapsiagaan sipil, pendidikan bela negara, dan penguatan keamanan digital (Raska & Bitzinger, 2022).

Dalam bidang pendidikan, indikator dapat mencakup jumlah lembaga pendidikan yang telah mengintegrasikan kurikulum bela negara, keterlibatan universitas dalam riset pertahanan nasional, serta terbentuknya program-program pelatihan kolaboratif antara pemerintah dan kampus (Setyawan & Rahardjo, 2022). Keterlibatan sektor swasta juga dapat dievaluasi melalui jumlah kemitraan strategis dalam pengembangan teknologi keamanan, pelatihan bersama, atau dukungan logistik nasional. Sebagai bagian dari evaluasi strategis, Indonesia dapat mengembangkan Indeks Ketahanan Nasional (IKN) yang menggabungkan seluruh indikator di atas dan diperbarui secara periodik oleh lembaga independen. Skema ini telah diadopsi oleh Finlandia dan Norwegia untuk memantau kesiapan nasional terhadap ancaman hybrid dan krisis sipil (Kivimaa et al., 2020). Dengan evaluasi yang kuat dan berkelanjutan, pemerintah tidak hanya dapat mengidentifikasi kelemahan dalam implementasi TDS, tetapi juga merancang kebijakan adaptif dan responsif yang mendorong sistem pertahanan nasional menuju arah yang lebih tangguh, kolaboratif, dan berorientasi jangka panjang.

Rekomendasi Implementatif dan Kebijakan Masa Depan

Berdasarkan evaluasi kesiapan nasional yang telah dijelaskan sebelumnya, terdapat beberapa rekomendasi implementatif yang dapat dijadikan dasar dalam merumuskan kebijakan penguatan *Total Defense System* (TDS) di Indonesia ke depan. “Rekomendasi ini bersifat multidimensional, berorientasi pada resiliensi jangka panjang, dan mempertimbangkan konteks geopolitik serta dinamika ancaman kontemporer yang semakin kompleks. Pertama, pembentukan lembaga nasional lintas sektoral khusus TDS yang memiliki kewenangan menyusun kebijakan, mengoordinasikan program, serta mengintegrasikan data dari kementerian dan lembaga terkait. Lembaga ini harus bertugas memastikan keselarasan antaragenda strategis seperti pertahanan digital, kesiapsiagaan bencana, ketahanan energi,

dan penguatan partisipasi masyarakat (Ericson et al., 2023). Kedua, penguatan kapasitas sumber daya manusia dalam pertahanan non-militer. Ini dapat dilakukan melalui pelatihan massal berbasis komunitas, program beasiswa studi strategis pertahanan untuk ASN dan generasi muda, serta pelatihan berjenjang bagi aparat daerah dan relawan bela negara (Setyawan & Rahardjo, 2022). Pemanfaatan pendekatan pelatihan berbasis simulasi dan digital juga harus ditingkatkan untuk memastikan adaptasi dengan bentuk-bentuk ancaman modern”. Ketiga, reformulasi anggaran pertahanan yang proporsional antara penguatan militer konvensional dan investasi pada dimensi non-militer seperti teknologi siber, kesehatan publik, dan pendidikan ketahanan nasional.

Kebijakan anggaran ini harus selaras dengan kerangka “Rencana Pembangunan Jangka Menengah Nasional (RPJMN) dan dapat disinergikan dengan Dana Desa, Dana Ketahanan Pangan, serta Dana Pemulihan Bencana untuk memperkuat basis pertahanan lokal (Wadjdi et al., 2024). Keempat, pengembangan ekosistem riset dan inovasi pertahanan nasional yang melibatkan perguruan tinggi, lembaga litbang pemerintah, industri pertahanan, dan startup teknologi. Indonesia harus mendorong program-program inkubasi teknologi untuk pertahanan siber, alat komunikasi darurat, sistem logistik otonom, serta pemodelan krisis berbasis AI (Wang & Xu, 2022). Pendanaan riset harus dijamin melalui skema matching fund antara pemerintah dan sektor swasta. Kelima, optimalisasi diplomasi pertahanan Indonesia dalam forum regional dan global, seperti ASEAN *Defence Ministers’ Meeting* (ADMM), QUAD+, dan *United Nations Peacekeeping*. Diplomasi ini harus difokuskan pada pengembangan interoperabilitas, pertukaran praktik terbaik dalam kesiapsiagaan sipil, serta penguatan jaringan *early warning system* dan sistem respons darurat lintas negara (Acharya, 2023; UN *Peacekeeping*, 2022). Terakhir, pembangunan sistem monitoring dan evaluasi nasional berbasis indikator digital, seperti dashboard kesiapan nasional yang real-time, indeks partisipasi publik terhadap bela negara, serta skor resiliensi daerah terhadap krisis multidimensi. Sistem ini akan memudahkan pengambilan keputusan berbasis data (*data-driven policy*) dan meningkatkan transparansi dalam pelaksanaan kebijakan pertahanan semesta” (Boin et al., 2022).

Melalui rekomendasi-rekomendasi strategis tersebut, Indonesia dapat membangun sistem pertahanan nasional yang adaptif, cerdas secara teknologi, kolaboratif secara sosial, dan berdaya saing di tingkat regional maupun global. TDS bukan sekadar kerangka kebijakan, tetapi fondasi penting dalam membangun masa depan ketahanan nasional yang kuat, berkelanjutan, dan partisipatif.

KESIMPULAN

Total Defense System merupakan pendekatan pertahanan yang mengintegrasikan seluruh elemen bangsa dalam menghadapi ancaman multidimensi, baik militer maupun non-militer. Dalam era “globalisasi dan kemajuan teknologi, ancaman terhadap keamanan nasional tidak lagi terbatas pada serangan fisik, tetapi juga mencakup serangan siber, pandemi, perubahan iklim, dan propaganda digital (Bergmann & Müller, 2021). Oleh karena itu, kebijakan pertahanan berbasis *Total Defense System* menjadi sangat relevan untuk diterapkan di Indonesia guna meningkatkan kesiapsiagaan nasional secara menyeluruh. *Total Defense System* memungkinkan mobilisasi sumber daya nasional secara efisien dan efektif dalam menghadapi berbagai krisis. Keberhasilan sistem ini bergantung pada koordinasi yang kuat antara pemerintah, sektor swasta, akademisi, dan masyarakat sipil dalam mengantisipasi serta menanggapi ancaman yang terus berkembang (Prakash et al., 2023). Implementasi kebijakan pertahanan ini tidak hanya berorientasi pada aspek militer, tetapi juga mencakup ketahanan ekonomi, ketahanan sosial, dan keamanan digital sebagai elemen utama dalam membangun resiliensi nasional (Ericson et al., 2023). Selain itu, “*Total Defense System* mendorong peningkatan literasi pertahanan bagi masyarakat. Pendidikan dan pelatihan kesiapsiagaan harus menjadi bagian dari kebijakan nasional agar seluruh warga negara memiliki pemahaman yang baik mengenai ancaman nasional serta cara untuk berkontribusi dalam mempertahankan stabilitas negara. Kesadaran dan keterlibatan aktif masyarakat dalam sistem pertahanan akan memperkuat solidaritas nasional serta menciptakan mekanisme perlindungan yang lebih efektif terhadap ancaman non-militer seperti disinformasi, sabotase ekonomi, dan serangan siber (Wadjdi et al., 2024). Implementasi *Total Defense System* telah banyak diterapkan di berbagai negara, sementara Indonesia masih menghadapi sejumlah tantangan dalam implementasinya. Tantangan utama meliputi kurangnya koordinasi lintas sektor dalam kebijakan pertahanan, keterbatasan anggaran, serta rendahnya partisipasi masyarakat dalam kesiapsiagaan nasional (Bergmann & Müller, 2021). Kurangnya integrasi kebijakan antar kementerian dan lembaga pertahanan menyebabkan tumpang tindih regulasi yang dapat menghambat efektivitas *Total Defense System*. Selain itu, alokasi anggaran yang lebih difokuskan pada penguatan militer konvensional seringkali

mengesampingkan pengembangan ketahanan siber dan kesiapsiagaan masyarakat (Prakash et al., 2023). Oleh karena itu, pemerintah perlu merancang strategi kebijakan yang lebih inklusif agar seluruh aspek pertahanan dapat berkembang secara seimbang. Rekomendasi utragetis untuk memperkuat implementasi *Total Defense System* di Indonesia memerlukan beberapa langkah yang dapat diterapkan meliputi: 1) Peningkatan kapasitas keamanan siber nasional. Indonesia harus mengalokasikan anggaran lebih besar untuk membangun infrastruktur keamanan digital dan sistem perlindungan data nasional (Ericson et al., 2023), 2) Edukasi dan pelatihan kesiapsiagaan masyarakat. Pemerintah perlu mengintegrasikan program literasi pertahanan dalam sistem pendidikan guna meningkatkan kesadaran dan keterlibatan publik dalam upaya pertahanan (Murfi et al., 2024), 3) Kerja sama internasional dalam pertahanan nasional. Indonesia perlu memperkuat kemitraan dengan negara-negara ASEAN dan mitra strategis global untuk meningkatkan kapabilitas pertahanan dan berbagi informasi intelijen (Wadjdi et al., 2024), 4) Pembangunan infrastruktur pertahanan yang tangguh. Investasi dalam ketahanan energi, ketahanan pangan, dan sistem logistik nasional menjadi prioritas guna menghadapi potensi krisis di masa depan. Dengan menerapkan langkah-langkah strategis ini, Indonesia dapat mengoptimalkan sistem pertahanannya serta memastikan kesiapan nasional dalam menghadapi ancaman global yang semakin kompleks. Oleh karena itu, *Total Defense System* memberikan landasan yang kuat bagi Indonesia untuk membangun sistem pertahanan nasional yang lebih modern, adaptif, dan tangguh terhadap ancaman multidimensi”. Dengan melibatkan seluruh elemen masyarakat dan mengintegrasikan berbagai sektor dalam strategi pertahanan, negara dapat meningkatkan ketahanan nasional secara signifikan. “Keberhasilan implementasi kebijakan ini bergantung pada komitmen pemerintah dalam menciptakan kebijakan yang terstruktur, investasi dalam penguatan sistem pertahanan, serta partisipasi aktif dari seluruh masyarakat. Melalui pendekatan ini, Indonesia dapat memastikan bahwa keamanan dan stabilitas nasional tetap terjaga di tengah perubahan global yang semakin dinamis”. Optimisme dan kolaborasi yang solid dari seluruh komponen bangsa baik pemerintah, stake holder terkait maupun masyarakat sangat penting dalam mewujudkan *Total Defense System* bagi bangsa Indonesia.

Referensi

- Acharya, A. (2023). *Constructing Global Order: Agency and Change in World Politics*. Cambridge University Press.
- Ahronheim, A. (2022). Youth military preparedness in Israel: Lessons from conscription culture. *Middle East Defense Review*, 27(2), 112–126.
- Barnea, S., & Harel, Y. (2021). Civic-military engagement in Israel's resilience strategy. *Journal of Strategic Studies*, 44(3), 410–428.
- Bergmann, J., & Müller, P. (2021). Learning to build resilience: The EU and the comprehensive approach to external crises. *Journal of Common Market Studies*, 59(6), 1347–1363. <https://doi.org/10.1111/jcms.13192>
- Boin, A., Ekengren, M., & Rhinard, M. (2022). *The EU as a crisis manager: Patterns and prospects*. Cambridge University Press.
- Chertoff, M., & Simon, T. (2021). The impact of deepfakes on democracy and security. *Journal of Cyber Policy*, 6(1), 20–39. <https://doi.org/10.1080/23738871.2021.1912819>
- Ericson, M., Wester, M., & Hammar, L. (2023). Sweden's Total Defence strategy: From vision to implementation. *Defense & Security Analysis*, 39(1), 41–59. <https://doi.org/10.1080/14751798.2023.2161910>
- Gillespie, M., & O'Loughlin, B. (2020). Strategic narratives in the age of disinformation. *International Affairs*, 96(6), 1461–1480. <https://doi.org/10.1093/ia/iaa169>
- Jensen, J. (2021). Nordic security governance and the role of interagency coordination. *Security Dialogue*, 52(5), 399–416. <https://doi.org/10.1177/0967010621995654>
- Kavakli, K. C., & Zhu, B. (2023). Resilience in authoritarian states: COVID-19 and beyond. *Political Science Quarterly*, 138(1), 115–140.
- Kivimaa, P., Boon, W., Hyysalo, S., & Klerkx, L. (2020). Towards a typology of intermediaries in sustainability transitions: A systematic review. *Environmental Innovation and Societal Transitions*, 36, 250–270. <https://doi.org/10.1016/j.eist.2020.07.001>
- Larsson, M. (2021). Building civilian preparedness for hybrid threats: Sweden's evolving model. *European Security*, 30(2), 280–298. <https://doi.org/10.1080/09662839.2021.1885936>
- Murfi, A., Pramudito, A., & Santosa, H. (2024). Evaluasi kebijakan pertahanan semesta Indonesia: Perspektif kelembagaan dan anggaran. *Jurnal Ketahanan Nasional*, 30(1), 55–74.
- Nesvetailova, A., & Palan, R. (2021). *Sabotage: The Hidden Nature of Finance*. Penguin Random House.
- Prakash, A., Wahyudi, A., & Thio, K. (2023). Rethinking cyber defense policies in ASEAN: Challenges and frameworks. *Asia-Pacific Journal of International Affairs*, 5(1), 77–95. <https://doi.org/10.1080/25741292.2023.2204011>
- Rainey, J., Allen, K., & Stenner, J. (2021). Digital infrastructure and strategic autonomy: The Nordic experience. *Defence Studies*, 21(4), 380–402.

- Raska, M., & Bitzinger, R. A. (2022). Security and defence transformation in small states: The case of Singapore. *The RUSI Journal*, 167(1), 76–90. <https://doi.org/10.1080/03071847.2022.2028875>
- Setyawan, D., & Rahardjo, T. (2022). Pendidikan bela negara dalam perspektif ketahanan nasional. *Jurnal Pertahanan Indonesia*, 8(2), 123–139.
- UN Peacekeeping. (2022). *Annual Report: United Nations Peacekeeping Operations*. <https://peacekeeping.un.org>
- Wajidi, F., Yulianti, N., & Rahmatullah, A. (2024). Kesiapsiagaan pertahanan masyarakat sipil terhadap ancaman siber. *Jurnal Pertahanan Siber Indonesia*, 3(1), 1–20.
- Wang, X., & Xu, Y. (2022). Artificial Intelligence and national security: A comparative perspective. *Journal of Strategic and Defense Studies*, 4(3), 201–225.
- Wong, A., Tan, C. H., & Lim, J. (2023). Building ASEAN's resilience: A roadmap for collaborative security. *Asia Security Review*, 18(2), 145–166.
- Wrange, P., Ekholm, D., & Löfgren, O. (2024). Civil-military synergy in Sweden's Totalförsvär model. *Scandinavian Journal of Military Studies*, 7(1), 88–105. <https://doi.org/10.31374/sjms.2024.03>