Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 3, Issue Agustus, 2025 pp. 19-29 http://urj.uin-malang.ac.id/index.php/mij/index

Analisis ketahanan nasional terhadap ancaman non-militer di era digital: tinjauan literatur strategi dan kebijakan di indonesia

Ainun Makkya Wahdania[1], Dewi zuhrotus Salwa[2], Dinda khumayra[3]
Program Studi Tadris Bahasa Inggris, Universitas Islam Negeri Maulana Malik Ibrahim Malang
*e-mail: *ainunmakkya598@gmail.com*

Kata Kunci:
Ketahanan Nasional; Ancaman Non Militer; Era Digital; Strategi Kebijakan; Indonesia
Keywords:
National Resilience; Non Militery Threats; Digital Age; Policy StrategyAge; Policy Strategy

A B S T R A K

Ketahanan nasional merupakan konsep strategis yang didalamnya mencakup upaya menjaga keutuhan dan stabilitas negara dalam menghadapi berbagai bentuk ancamanntermasuk ancaman non-militer yang berkembang pesat di era digital. Penelitian ini bertujuan untuk mengkaji respons dan strategi ketahanan nasional Indonesia dalam menghadapi tantangan kontemporer seperti disinformasi ataupun polarisasi sosial, serangan siber, serta disrupsi teknologi informasi. Metode yang digunakan dalam penelitian ini yakni kualitatif dengan pendekatan literatur review berbasis normatif-konseptual dan analisis deskriptif. Data dikumpulkan melalui telaah sistematis terhadap kebijakan pemerintah, jurnal ilmiah, dokumen resmi nasional, serta publikasi internasional yang relevan. Hasil kajian menunjukkan bahwa pendekatan multidimensi dalam ketahanan nasional meliputi aspek digital literacy, regulasi keamanan siber, dan penguatan kohesi sosial yang sangat diperlukan untuk menghadapi spektrum ancaman baru yang bersifat non konvensional. Adapun penelitian ini merekomendasikan peningkatan kapasitas kelembagaan dan kolaborasi lintas sektor sebagai bagian dari reformulasi strategi ketahanan nasional yang adaptif dan berkelanjutan di era digital.

A B S T R A C T

National resilience is a strategic concept that includes efforts to maintain the integrity and stability of the state in the face of various forms of threats, including non-military threats that are growing rapidly in the digital era. This research aims to examine Indonesia's national resilience responses and strategies in facing contemporary challenges such as disinformation or social polarization, cyber attacks, and information technology disruption. The method used in this research is qualitative with a normative-conceptual-based literature review approach and descriptive analysis. Data was collected through a systematic review of government policies, scientific journals, national official documents, and relevant international publications. The results of the study show that a multidimensional approach to national resilience includes aspects of digital literacy, cybersecurity regulation, and strengthening social cohesion which are needed to deal with a new spectrum of unconventional threats. This study recommends increasing institutional capacity and cross-sector collaboration as part of the reformulation of an adaptive and sustainable national resilience strategy in the digital era.

Pendahuluan

Kemampuan suatu negara untuk bertahan dan beradaptasi terhadap ancaman dalam dan luar negeri dikenal sebagai ketahanan nasional. Ancaman-ancaman ini dapat mencakup agresi militer, konflik sosial, atau bencana alam. Oleh karena itu, ketahanan

nasional harus ditanamkan dan diinternalisasikan dalam semua aspek kehidupan masyarakat, sehingga setiap orang memahami peran dan tanggung jawab mereka dalam menjaga stabilitas dan keamanan negara. Perkembangan teknologi informasi dan komunikasi dalam dua dekade terakhir telah membawa dunia memasuki era digital yang penuh disrupsi. Meskipun adanya kemajuan ini telah menciptakan efisiensi, konektivitas, dan transformasi di berbagai sektor namun pada saat yang sama juga menghadirkan bentuk ancaman baru yang bersifat non-militer dan sulit dideteksi secara konvensional. Ancaman seperti serangan siber disinformasi, hoaks, radikalisme digital, serta polarisasi sosial melalui media sosial menjadi tantangan serius terhadap stabilitas sosial-politik dan ketahanan nasional negara-negara di seluruh dunia (). Bahkan pada era ini, kekuatan negara tidak lagi semata ditentukan oleh kekuatan militer akan tetapi juga oleh kapasitasnya dalam merespons ancaman asimetris yang bersifat ideologis dan teknologi.

Di Indonesia, adanya fenomena banyak sekali ditemukan dalam kehidupan sehari-hari seperti adanya berita hoax maupun ancaman cyber. Hal ini diperkuat berdasarkan laporan Badan Siber dan Sandi Negara (BSSN) sepanjang tahun 2023 terjadi lebih dari 400 juta anomali trafik siber yang mengindikasikan potensi serangan terhadap sistem informasi nasional. Di sisi lain adanya penyebaran disinformasi meningkat pesat menjelang tahun politik 2024 yang menyebabkan tingginya eskalasi konflik identitas, degradasi kohesi sosial, serta penurunan kepercayaan publik terhadap institusi negara (BSSN, 2024). Indeks Ketahanan Sosial Nasional yang dirilis oleh Kementerian Dalam Negeri juga menunjukkan tren penurunan dalam hal kepercayaan antar kelompok masyarakat terutama di wilayah perkotaan yang padat interaksi digital (Kemendagri, 2024). Sehingga dapat menjadi indikator penting bahwa ketahanan nasional Indonesia tengah diuji tidak hanya oleh ancaman fisik eksternal akan tetapi oleh dinamika internal yang bersifat non-militer.

Di tengah tantangan tersebut adanya konsep ketahanan nasional perlu dipahami secara holistik sebagai upaya kolektif bangsa untuk menjaga eksistensi dan integritas nasional dari berbagai bentuk gangguan baik yang bersifat konvensional maupun non-konvensional. Dalam paradigma baru ini adanya pertahanan tidak lagi hanya tugas TNI melainkan menjadi tanggung jawab bersama yang melibatkan masyarakat sipil, pemerintah, sektor swasta, dan dunia pendidikan. Ditambah lagi adanya ketahanan informasi, ketahanan budaya, ketahanan ekonomi, dan ketahanan moral yang menjadi unsur penting dalam memperkuat daya tahan bangsa. Ketahanan nasional yang hanya bertumpu pada aspek militer tidak lagi relevan di era digital yang serba cepat dan kompleks.

Adapun beberapa literatur mengenai ketahanan nasional pada umumnya masih banyak berfokus pada aspek fisik atau militeristik sementara kajian terhadap bentuk-bentuk ancaman non-militer masih terbatas dan belum sepenuhnya dikembangkan dalam kerangka kebijakan yang adaptif. Padahal dalam realitas kontemporer, ancaman seperti infiltrasi ideologis melalui media sosial, manipulasi opini publik berbasis algoritma, serta perang narasi digital menjadi alat strategis bagi pihak asing maupun aktor non-negara untuk melemahkan kedaulatan suatu bangsa tanpa kontak senjata. Kondisi ini menuntut adanya reformulasi strategi ketahanan nasional yang mampu

merespons tantangan digital secara responsif, komprehensif, dan kontekstual.

Beberapa penelitian terdahulu telah membahas ketahanan nasional dari berbagai sudut pandang. Salah satunya pada penelitian yang dilakukan oleh (Widodo,n2021) yang menekankan pentingnya kesiapsiagaan militer dalam menjaga kedaulatan negara sementara studi (Syamsudin, 2022) lebih menyoroti dimensi ideologis dalam menghadapi radikalisme. Sementara itu, penelitian (Wahyuni dan Rahman,!2023) mengkaji potensi ancaman siber di sektor pemerintahan namun belum mengaitkannya dengan strategi kebijakan ketahanan nasional secara menyeluruh. Di sisi lain, kajian oleh Herlambang (2024) menyebut bahwa respons Indonesia terhadap disinformasi masih bersifat sektoral dan minim koordinasi antarlembaga.

Hal ini sejalan dengan kebutuhan akan pendekatan yang lebih integratif dan literatur yang mampu menjembatani pemahaman konseptual dan praktik kebijakan dalam menghadapi ancaman non-militer secara kontemporer. Sehingga dengan adanya penelitian ini dapat mengisi kesenjangan tersebut dengan menelaah secara sistematis strategi dan kebijakan ketahanan nasional Indonesia terhadap ancaman non-militer di era digital berdasarkan tinjauan literatur yang komprehensif.Selain itu, lemahnya literasi digital masyarakat dan terbatasnya regulasi terhadap konten digital yang bermuatan provokatif semakin memperburuk situasi. Berdasarkan survei APJII tahun 2024, sebanyak 58% pengguna internet di Indonesia belum mampu membedakan informasi faktual dan hoaks secara mandiri. Hal ini membuka celah bagi berkembangnya intoleransi ataupun ujaran kebencian serta radikalisasi daring yang mengancam persatuan nasional. Ditambah lagi regulasi yang ada masih bersifat sektoral dan reaktif, sementara upaya integratif lintas kementerian belum berjalan efektif. Sehingga adanya ketahanan nasional di era digital menuntut kehadiran strategi kebijakan yang berbasis nilai, literasi, dan partisipasi publik yang luas.

Fenomena tersebut menunjukkan bahwa ancaman non-militer memiliki karakteristik yang sangat dinamis dan kompleks. Dalam hal ini adanya strategi ketahanan nasional tidak dapat lagi berorientasi semata pada pertahanan fisik melainkan harus mampu menjawab persoalan-persoalan yang menyangkut identitas dan keamanan digital masyarakat. Ditambah lagi adanya strategi nasional harus dirumuskan tidak hanya oleh aktor negara akan tetapi juga dengan pelibatan multisektor untuk menciptakan ketahanan yang berlapis (layered resilience). Karena pada dasarnya tanpa keterlibatan masyarakat dan infrastruktur kebijakan yang adaptif maka sebuah negara akan terus tertinggal dalam merespons ancaman yang terus berubah wujud dan pola.

Oleh karena itu, dari latar belakang tersebut tujuan dari penulisan ini untuk melakukan kajian mendalam mengenai relevansi dan efektivitas strategi ketahanan nasional dalam menghadapi ancaman non-militer di era digital,l dengan menelaah berbagai literatur akademik dan kebijakan nasional yang ada. Dengan demikian penelitian ini diharapkan dapat memberikan kontribusi ilmiah terhadap pengembangan kerangka kebijakan ketahanan nasional yang lebih kontekstual, integratif, dan berbasis realitas digital Indonesia saat ini sekaligus memperkuat daya tahan bangsa dari dalam melalui pendekatan strategis yang holistik.

Metode

Penelitian ini menggunakan metode kualitatif dengan pendekatan kajian kepustakaan (library research) yang berorientasi pada analisis konseptual. Metode ini dipilih untuk mengkaji secara mendalam konsep ketahanan nasional dalam menghadapi ancaman non-militer di era digital serta menganalisis strategi dan kebijakan yang telah dan sedang diterapkan oleh pemerintah Indonesia. Adapun pendekatan yang digunakan dalam penelitian ini difokuskan pada studi literatur sebagai sumber utama dalam menelaah dinamika ancaman kontemporer serta respons kebijakan yang muncul sebagai upaya mitigasi dan penguatan ketahanan nasional secara menyeluruh.Sumber data dalam penelitian ini diperoleh dari bahan pustaka primer dan sekunder. Bahan primer meliputi dokumen resmi kebijakan pemerintah seperti Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, dokumen Rencana Induk Ketahanan Nasional, Perpres tentang Keamanan Siber, serta Rencana Pembangunan Jangka Menengah Nasional (RPJMN) yang memuat isu ketahanan informasi, keamanan siber, dan perlindungan ruang digital. Bahan sekunder terdiri dari jurnal ilmiah nasional dan internasional yang terindeks Scopus dan Sinta, buku kajian strategis, laporan dari lembaga riset seperti BSSN, Kemenhan, dan LIPI, serta artikel analisis kebijakan yang membahas tantangan dan strategi ketahanan non-militer di Indonesia.

Teknik pengumpulan data dilakukan melalui penelusuran literatur secara sistematis menggunakan kata kunci seperti "ketahanan nasional digital", "non-military threats", "cybersecurity policy Indonesia", "disinformasi digital", dan "kebijakan keamanan nasional" melalui database seperti Scopus, Google Scholar, DOAJ, Sinta, serta dokumen resmi pemerintah. Sehingga nantinya peneliti juga menelaah laporan tahunan lembaga-lembaga strategis dan regulasi nasional yang berkaitan dengan keamanan informasi dan perlindungan data.Adapun terkait analisis data dilakukan dengan metode deskriptif kualitatif melalui pendekatan analitis komparatif. Dimana nantinya peneliti membandingkan berbagai model strategi dan kebijakan ketahanan nasional terhadap ancaman non militer baik di Indonesia maupun dari beberapa negara lain sebagai studi perbandingan. Fokus analisis diarahkan pada isu-isu seperti disinformasi, polarisasi opini publik, keamanan data, serta ancaman ideologis digital yang berdampak pada stabilitas nasional. Kerangka analisis mengacu pada teori ketahanan nasional, konsep keamanan manusia (human security) serta pendekatan strategis berbasis tata kelola digital.

Penalaran yang digunakan bersifat deduktif yaitu dimulai dari kajian teoritis tentang konsep ketahanan nasional dan klasifikasi ancaman non-militer yang kemudian diturunkan pada konteks kebijakan strategis dan kelembagaan yang diterapkan di Indonesia. Sehingga melalui pendekatan literatur yang komprehensif maka penelitian ini diharapkan dapat memberikan kontribusi teoritis dan praktis dalam pengembangan model ketahanan nasional yang responsif terhadap dinamika ancaman digital serta mendukung penguatan strategi kebijakan yang adaptif, partisipatif, dan terintegrasi.

Hasil dan Pembahasan

Tata kelola Ketahanan nasional merupakan fondasi utama dalam menjamin keberlangsungan kehidupan berbangsa dan bernegara. Dalam konteks era digital yang semakin kompleks adanya ancaman terhadap ketahanan nasional tidak hanya datang dari aspek militer, namun juga dari ancaman non-militer yang bersifat multidimensional seperti disinformasi, serangan siber, degradasi budaya, ancaman terhadap kedaulatan data hingga degradasi moral generasi muda akibat paparan digital yang tidak terkontrol. Sehingga sangat penting untuk memahami dinamika ancaman non-militer di era digital dan bagaimana strategi serta kebijakan nasional merespons hal tersebut.

Pengertian dan Pilar Utama Ketahanan Nasional

Ketahanan nasional adalah kondisi dinamis bangsa dalam menghadapi berbagai ancaman, tantangan, hambatan, dan gangguan (ATHG) yang berasal dari dalam maupun luar negeri guna menjaga keutuhan, kedaulatan, dan kelangsungan hidup negara. Pada dasarnya ketahanan nasional Indonesia mengacu pada delapan aspek kehidupan nasional yang dikenal sebagai Astagatra yakni tiga gatra alamiah (geografi, demografi, dan sumber kekayaan alam) serta lima gatra sosial (ideologi, politik, ekonomi, sosial budaya, dan pertahanan keamanan). Dalam era digital adanya peran ketahanan nasional perlu dibingkai ulang dengan mempertimbangkan perubahan lanskap geopolitik ataupun kemajuan teknologi informasi dan meningkatnya peran ruang siber sebagai domain strategis baru dalam kompetisi global. Karena itu sebuah negara tidak hanya harus membangun ketahanan fisik dan militer akan tetapi juga memperkuat pertahanan kognitif dan sosial masyarakat.

Ancaman Non-Militer di Era Digital

Terdapat beberapa ancaman non militer yang sering kali terjadi diantara:

Disinformasi dan Manipulasi Opini Publik

Salah satu bentuk ancaman non-militer yang paling menonjol di era digital adalah penyebaran disinformasi dan hoaks. Teknologi informasi memungkinkan aktor non-negara maupun negara untuk menyebarkan narasi palsu, membentuk opini publik secara masif, dan memecah belah masyarakat. Ditambah lagi adanya serangan semacam ini telah terjadi dalam berbagai bentuk mulai dari propaganda politik hingga kampanye hitam terhadap institusi negara.

Serangan Siber terhadap Infrastruktur Strategis

Ancaman siber terhadap infrastruktur penting seperti sistem perbankan, pembangkit listrik, sistem transportasi, dan data pemerintah merupakan bentuk ancaman nyata yang bisa melumpuhkan stabilitas nasional. Kasus peretasan terhadap data pribadi penduduk atau situs-situs lembaga negara seperti yang pernah dialami Komisi Pemilihan Umum (KPU) dan BSSN menjadi alarm penting bagi ketahanan digital nasional.

Kedaulatan Data dan Dominasi Platform Global

Platform digital global seperti Google, Facebook, dan TikTok memiliki kontrol besar atas arus informasi dan data masyarakat Indonesia. Hal ini menimbulkan persoalan

serius terkait kedaulatan data karena negara kehilangan kendali atas informasi strategis yang bisa berdampak pada keamanan nasional. Lebih lanjut, adanya praktik ekonomi digital yang didominasi oleh perusahaan luar negeri juga berisiko melemahkan ketahanan ekonomi digital domestik.

Degradasi Budaya dan Moral

Di zaman sekarang, akhlak dan moral remaja semakin merosot, terlihat dari maraknya pergaulan bebas, hamil di luar nikah, hingga kebiasaan mabuk-mabukan. Hal ini terjadi karena minimnya pengetahuan dan pengamalan agama. Jika dibiarkan, masalah ini tidak hanya merusak masa depan generasi muda, tetapi juga melemahkan ketahanan nasional karena kualitas sumber daya manusia menjadi rapuh dan rentan terhadap pengaruh negatif globalisasi.Arus globalisasi budaya melalui media sosial dan platform streaming berkontribusi pada pergeseran nilai, gaya hidup konsumtif, serta pola pikir instan. Dimana adanya fenomena ini menyebabkan terjadinya disorientasi budaya dan hilangnya identitas nasional terutama di kalangan generasi muda. Ketahanan sosial budaya menjadi rentan ketika konten-konten asing yang tidak sejalan dengan nilai luhur bangsa lebih dominan dikonsumsi oleh masyarakat.

Radikalisme Digital dan Polarisasi Sosial

Radikalisme digital adalah sebuah ideologi yang menginginkan perubahan atau pembaharuan secara digital melalui cara-cara kekerasan, kejam, dan ekstrem. Ruang digital juga menjadi sarana penyebaran ideologi ekstrem dan radikalisme baik berbasis agama maupun politik. Dengan algoritma media sosial yang memperkuat echo chamber maka masyarakat rentan mengalami polarisasi sosial yang mengganggu integrasi nasional. Konten provokatif dan ujaran kebencian dapat dengan cepat menyebar dan memicu konflik horizontal. Karena itu, diperlukan penguatan berpikir kritis, nilai kebangsaan, dan pemahaman agama seimbang agar milenial mampu menolak pengaruh radikalisme digital.

Strategi Nasional dalam Menghadapi Ancaman Non-Militer

Dari adanya fenomena tersebut maka untuk menghadapi kompleksitas ancaman non-militer di era digital pemerintah Indonesia telah menyusun berbagai strategi dan kebijakan meskipun belum sepenuhnya terintegrasi dalam satu kerangka ketahanan nasional digital. Mulai dari pertama, strategi siber nasional dimana peran pemerintah melalui Badan Siber dan Sandi Negara (BSSN) telah menetapkan Strategi Keamanan Siber Nasional untuk memperkuat sistem keamanan informasi nasional termasuk pengamanan infrastruktur kritis. Di samping itu, UU Perlindungan Data Pribadi (PDP) tahun 2022 menjadi tonggak penting dalam menjamin hak-hak digital warga negara dan memperkuat kedaulatan data nasional. (BSSN, 2022). Kedua, peran literasi digital dan pendidikan karakter, terlebih lagi dikarenakan kementerian Komunikasi dan Informatika (Kominfo) meluncurkan program Gerakan Nasional Literasi Digital sebagai upaya membangun ketahanan individu dan masyarakat terhadap hoaks, ujaran kebencian, dan konten negatif lainnya. Namun, adanya efektivitas program ini masih perlu ditingkatkan melalui integrasi dengan kurikulum pendidikan formal dan partisipasi aktif masyarakat sipil.

Ketiga, adanya regulasi media sosial dan konten digital dimana sebuah kebijakan moderasi konten yang diatur dalam Permenkominfo No. 5 Tahun 2020 tentang Penyelenggaraan Sistem Elektronik menjadi instrumen untuk menekan penyebaran konten berbahaya. Namun, tantangan besar masih dihadapi terkait transparansi platform digital dan perlindungan terhadap kebebasan berekspresi. Keempat, adanya kebijakan ketahanan sosial budaya pemerintah melalui Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi berupaya memperkuat nilai-nilai kebangsaan melalui program penguatan karakter dan pelestarian budaya lokal. Namun di era digital maka diperlukan strategi kebudayaan yang adaptif dengan teknologi dan berbasis komunitas digital. Terakhir, adanya kolaborasi multipihak dalam ketahanan digital dimana dengan adanya ketahanan nasional di era digital bukan hanya tanggung jawab pemerintah akan tetapi juga memerlukan keterlibatan sektor swasta, media, akademisi, dan masyarakat sipil. Kolaborasi multipihak diperlukan untuk membangun sistem peringatan dini digital, edukasi publik yang inklusif dan penguatan ekosistem teknologi lokal.

Kritik dan Tantangan Implementasi

Meskipun sejumlah strategi telah dijalankan, terdapat berbagai tantangan yang menghambat efektivitasnya seperti: kurangnya koordinasi antar lembaga dalam menangani isu digital secara lintas sektor, keterbatasan sumber daya manusia di bidang keamanan siber dan literasi digital, adanya tumpang tindih regulasi yang menimbulkan ketidakpastian hukum dan membuka celah pelanggaran hak digital, dan rendahnya kesadaran masyarakat terhadap urgensi ancaman non-militer dan pentingnya ketahanan digital. Ditambah lagi adanya ketahanan nasional digital juga menghadapi tantangan dari aspek struktur birokrasi yang belum adaptif terhadap dinamika dunia digital. Dimana banyak lembaga pemerintah masih bekerja secara sektoral dan hierarkis yang membuat respons terhadap ancaman digital seperti disinformasi, serangan siber, dan penyebaran ujaran kebencian yang menjadi lambat dan terfragmentasi. Tidak adanya single authority yang secara khusus memiliki mandat penuh menangani keamanan digital nasional juga mengakibatkan lemahnya pengambilan keputusan yang terkoordinasi dan terpadu.

Adanya kritik juga muncul terhadap regulasi yang bersifat reaktif dan belum komprehensif. Misalnya saja pada Undang-Undang ITE yang sering menjadi perdebatan karena multitafsir dan dinilai mengancam kebebasan sipil yang menunjukkan bahwa pendekatan regulatif terhadap ruang digital masih belum seimbang antara aspek keamanan dan perlindungan hak warga negara. Hal ini menjadi paradoks ketika negara berupaya meningkatkan ketahanan nasional tetapi justru menciptakan distrust publik terhadap instrumen hukumnya. Di sisi lain, adanya tantangan besar terletak pada kesenjangan digital antarwilayah. Ketimpangan akses internet antara kota besar dan daerah tertinggal membuat pembangunan ketahanan nasional digital tidak berjalan merata. Masyarakat di daerah yang belum terkoneksi internet secara optimal menjadi kelompok rentan terhadap manipulasi informasi, propaganda daring, hingga penipuan digital. Hal ini mencerminkan bahwa ketahanan digital bukan hanya soal teknologi, tetapi juga soal keadilan distribusi infrastruktur.

Terakhir, adanya keterlibatan masyarakat sipil dan sektor non-pemerintah masih sangat terbatas. Padahal, untuk menciptakan ketahanan nasional yang menyeluruh,

diperlukan partisipasi aktif dari berbagai pemangku kepentingan seperti komunitas digital, akademisi, pelaku industri teknologi, dan media. Serta minimnya kolaborasi multisektor menyebabkan strategi yang diterapkan kurang responsif terhadap kebutuhan lapangan, tidak fleksibel, dan sering kali ketinggalan dibandingkan kecepatan disrupsi digital itu sendiri. Dengan demikian, meskipun Indonesia telah menunjukkan kemajuan dalam merancang kebijakan ketahanan digital akan tetapi adanya kritik dan tantangan di atas menunjukkan perlunya pembaruan pendekatan yang lebih kolaboratif dan berbasis masyarakat. Karena pada dasarnya ketahanan nasional di era digital tidak dapat dibangun hanya oleh negara akan tetapi harus menjadi agenda bersama seluruh elemen bangsa.

Rekomendasi Implementatif

Sehingga dari adanya fenomena tersebut maka hasil kajian menunjukkan untuk meningkatkan ketahanan nasional terhadap ancaman non-militer di era digital, beberapa rekomendasi penting antara lain:

1. Membangun kerangka kebijakan ketahanan nasional digital yang holistik dan terintegrasi dengan dokumen strategis nasional seperti RPJPN dan RPJMN.
2. Memperkuat kapasitas kelembagaan dan sumber daya manusia di bidang keamanan siber dan literasi digital melalui pelatihan berkelanjutan.
3. Mengembangkan algoritma lokal dan ekosistem digital mandiri untuk mengurangi ketergantungan pada platform global.
4. Meningkatkan kesadaran masyarakat melalui pendekatan budaya digital berbasis lokalitas dan nilai-nilai Pancasila.
5. Mendorong transparansi dan akuntabilitas platform digital melalui kerja sama bilateral dan multilateral.

Karena pada dasarnya ketahanan nasional dalam menghadapi ancaman non-militer di era digital menuntut paradigma baru dalam merespons dinamika global dan lokal yang terus berubah. Dimana sebuah negara perlu membangun ketahanan yang adaptif dan inklusif tidak hanya melalui pendekatan regulatif, tetapi juga dengan memperkuat etika digital, kesadaran kolektif, dan partisipasi aktif masyarakat dalam menjaga keutuhan bangsa. Oleh karena itu, ketahanan nasional bukanlah tugas eksklusif militer dan pemerintah akan tetapi merupakan tanggung jawab bersama seluruh elemen bangsa di era digital yang sarat dengan tantangan tak kasat mata namun sangat nyata.Berbagai studi literatur menunjukkan bahwa paradigma ketahanan nasional dewasa ini tidak lagi dapat dipisahkan dari dinamika ancaman non-militer khususnya di era digital. Adanya ketahanan nasional tidak lagi dipahami semata sebagai kemampuan pertahanan dalam arti militeristik akan tetapi sebagai sistem menyeluruh yang mencakup kekuatan ideologis, ekonomi, sosial-budaya, politik, serta keamanan siber. Dalam konteks ini ancaman non-militer seperti disinformasi digital berupa serangan siber terhadap infrastruktur vital, infiltrasi ideologi transnasional melalui media sosial hingga ketimpangan akses teknologi telah menjadi tantangan serius terhadap stabilitas negara.

Hal ini sejalan dengan penelitian yang dilakukan oleh Marfi (2024) yang menyoroti bahwa ketahanan nasional Indonesia berada dalam posisi rentan akibat lemahnya

regulasi digital dan koordinasi antar lembaga dalam merespons ancaman non-fisik. Studi ini menegaskan bahwa arsitektur kelembagaan di bidang keamanan informasi di Indonesia masih bersifat sektoral dan tidak terintegrasi. Akibatnya dalam beberapa kasus seperti kebocoran data publik atau penyebaran hoaks berskala besar negara terlambat dalam mengambil tindakan preventif maupun responsif. Hal ini diperkuat oleh temuan (Alfi, 2023) yang menggarisbawahi bahwa rendahnya literasi digital di kalangan masyarakat memperbesar peluang polarisasi sosial akibat manipulasi opini publik melalui media digital.

Lebih lanjut adanya ancaman non-militer yang bersifat ideologis juga menjadi fokus perhatian dalam kajian strategis nasional. Penelitian (Kashuri, 2024) menemukan bahwa era digital telah memfasilitasi penyebaran paham radikalisme dan intoleransi dengan cara yang lebih masif cepat, dan sulit dilacak. Media sosial menjadi arena baru penyebaran narasi-narasi yang merongrong nilai-nilai kebangsaan seperti Pancasila, dan integrasi sosial. Dalam kondisi ini adanya strategi ketahanan nasional tidak bisa mengandalkan pendekatan koersif semata melainkan menuntut keterlibatan aktif dari masyarakat sipil dimana sebuah lembaga pendidikan, dan tokoh agama dalam membangun kesadaran kolektif.Dalam kerangka ketahanan nasional yang berkelanjutan maka adanya pendekatan strategis yang inklusif dan berbasis nilai-nilai kebangsaan menjadi sangat krusial. Hal ini diketahui diperkuat oleh studi yang dilakukan oleh (Sa'diyah, 2016) menegaskan pentingnya integrasi antara strategi pertahanan siber dan penguatan karakter kebangsaan (nationhood). Peneliti menyebut bahwa ketahanan nasional digital hanya dapat dicapai bila negara tidak hanya memperkuat infrastruktur teknologi akan tetapi juga memperkuat ideologi melalui pendidikan kewargaan yang kritis dan adaptif terhadap zaman. Dengan demikian, tantangan ketahanan nasional bukan semata isu teknis, melainkan menyangkut pembangunan jangka panjang atas watak bangsa yang resilien secara sosial dan ideologis.

Kesimpulan

Penelitian ini menyimpulkan bahwa ketahanan nasional terhadap ancaman non-militer di era digital merupakan isu strategis yang menuntut respons kebijakan yang adaptif, integratif, dan berkelanjutan. Dimana terdapat beberapa ancaman seperti disinformasi, serangan siber, degradasi budaya nasional, hingga polarisasi sosial melalui media digital telah melampaui batas keamanan tradisional dan memerlukan pendekatan keamanan nasional yang multidimensional. Strategi ketahanan yang efektif tidak hanya bergantung pada kemampuan teknologi akan tetapi juga pada tata kelola yang kolaboratif serta edukasi publik yang berkelanjutan.Hasil kajian menunjukkan bahwa penguatan ketahanan nasional di ranah non-militer memerlukan sinergi lintas sektor, reformasi regulasi digital, serta revitalisasi nilai kebangsaan dalam ruang maya. Dimana strategi dan kebijakan yang berbasis literatur dan best practice jika diimplementasikan secara konsisten dapat menjadi fondasi untuk menjaga stabilitas negara dan integritas sosial-politik di tengah era disrupsi informasi. Oleh karena itu, adanya integrasi pendekatan literatur strategis dan kebijakan adaptif pada dasarnya sangat diperlukan untuk membentuk arsitektur ketahanan nasional yang kokoh dan kontekstual terhadap

dinamika ancaman digital masa kini.

Saran

Penulis menyadari bahwa artikel ini masih memiliki keterbatasan baik dari segi cakupan kajian maupun kedalaman analisis. Oleh karena itu, penulis sangat mengharapkan saran dan masukan konstruktif dari pembaca sebagai upaya untuk menyempurnakan tulisan ini di masa mendatang. Semoga artikel ini dapat memberikan kontribusi awal dalam pengembangan kajian ketahanan nasional khususnya dalam menghadapi ancaman non-militer di era digital.

Daftar Pustaka

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 6(2), 5

Darumaya, B. A., Maarif, S., Toruan, T., & Swastanto, Y. (2023). Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan. Jurnal Keamanan Nasional, 9(2), 299-324.

Hartono, D. (2020). Fenomena kesadaran bela negara di era digital dalam perspektif ketahanan nasional. Jurnal Lemhannas RI, 8(1), 14-33.

Estika, F., Sumarno, A. P., & Al-Mubaroq, H. Z. (2024). PERAN STRATEGIS KOMPONEN CADANGAN DALAM SISTEM PERTAHANAN SEMESTA INDONESIA: TANTANGAN DAN PELUANG. Bussman Journal: Indonesian Journal of Business and Management, 4(3), 1202-1213.

Fanani, A., Midhio, I. W., & Hendra, A. (2024). TANTANGAN PERTAHANAN NASIONAL MENUJU INDONESIA EMAS 2045. TheJournalish: Social and Government, 5(4), 379-391.

Kashuri, M. (2024). BENCHMARK KEBIJAKAN PERTAHANAN NON MILITER DARI BERBAGAI NEGARA: SEBUAH REVIEW. JISIP UNJA (Jurnal Ilmu Sosial Ilmu Politik Universitas Jambi), 149-158.

Murfi, Y. (2024). Sishankamrata: Analisis komprehensif sistem pertahanan dan keamanan Indonesia terpadu dalam perspektif sejarah. Jurnal Ilmu Pendidikan (ILPEN), 3(1), 24-45.

Purwantoro, S. A. (2020). Mempersiapkan Sumber Daya Manusia Kritis, Kreatif, dan Berwawasan Kebangsaan untuk Mencapai Ketahanan Nasional yang Tangguh Di Era Pandemik Covid-19. Jurnal Lemhannas RI, 8(2), 151-169.

Putri, R. A. (2019). Perancangan SLA (Service Level Agreement) SIAKAD Berdasarkan Kerangka Kerja CMMI-SVC dan ITIL V3 (Studi Kasus: UIN Malang) (Doctoral dissertation, Institut Teknologi Sepuluh Nopember).

Pratama, R., Timur, F. G. C., & Sutanto, R. (2023). Revitalisasi kewaspadaan nasional melalui sistem pertahanan dan keamanan terhadap ancaman perang asimetris. Nusantara: Jurnal Ilmu Pengetahuan Sosial, 10(9), 4548-4559.

Rasji, R., Rohma, I. A., Imanto, K. S. M., & Yandika, N. P. (2024). Tinjauan Peran Pemimpin Indonesia dalam Membangun Ketahanan Negara. Innovative: Journal Of Social Science Research, 4(2), 8283-8289.

Sa'diyah, N. K., & Vinata, R. T. (2016). Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara. Perspektif: Kajian Masalah Hukum Dan Pembangunan, 21(3), 168-187.

Yanuarti, I., Wibisono, M., & Midhio, I. W. (2020). Strategi Kerja Sama Indo-Pasifik Untuk Mendukung Pertahanan Negara: Perspektif Indonesia. Strategi Perang Semesta, 6(1).https://urj.uinmalang.ac.id/index.php/mij/article/download/9818/3870/?utm_source=chatgpt.com