

**URGENSI KETAHANAN BANGSA DALAM MENGHADAPI PERANG ASIMETRIS;
ANCAMAN PEMIKIRAN DAN SERANGAN DIGITAL**

Fuad¹, Rio Ramabaskara²

Email : ¹sangfuad2018@gmail.com, ²adv.ramabaskara@gmail.com

¹Fakultas Hukum Universitas Widya Mataram, ²Universitas Al Azhar Indonesia

Abstrak

Perang asimetris telah menjelma menjadi bentuk ancaman strategis yang tidak lagi bergantung pada kekuatan militer, melainkan melalui manipulasi informasi, serangan digital, dan infiltrasi ideologis. Penelitian ini bertujuan untuk menganalisis strategi ketahanan bangsa Indonesia dalam merespons ancaman pemikiran dan serangan digital yang terstruktur dan sistematis. Menggunakan pendekatan normatif-empiris dengan teknik analisis kualitatif, artikel ini mengkaji dinamika perang asimetris dalam ranah ideologi dan teknologi informasi, serta mengevaluasi kapasitas kelembagaan dan kebijakan nasional. Temuan menunjukkan bahwa ketahanan bangsa memerlukan sinergi antara pemerintah, masyarakat sipil, dan sektor pendidikan dalam memperkuat literasi digital, perlindungan ideologi Pancasila, dan pembangunan sistem keamanan informasi yang adaptif. Evaluasi terhadap strategi nasional juga mengindikasikan perlunya koordinasi antar-lembaga, peningkatan kapasitas SDM, serta regulasi yang progresif namun berimbang terhadap hak sipil. Dengan memperkuat ketahanan ideologis dan digital secara menyeluruh, Indonesia dapat mempertahankan kedaulatan dan stabilitas nasional di tengah eskalasi perang asimetris global.

Kata Kunci: Perang, Ideologi, Asimetris, Digital, Siber

Abstract

Asymmetric warfare has evolved into a form of strategic threat that no longer relies solely on military power, but rather operates through information manipulation, cyberattacks, and ideological infiltration. This study aims to analyze Indonesia's national resilience strategies in responding to structured and systematic ideological threats and digital attacks. Employing a normative-empirical approach with qualitative analysis techniques, this article examines the dynamics of asymmetric warfare within the domains of ideology and information technology, while evaluating the capacity of national institutions and policies. The findings indicate that national resilience requires synergy among the government, civil society, and the education sector in strengthening digital literacy, safeguarding the ideology of Pancasila, and developing adaptive information security systems. An evaluation of national strategies also highlights the need for inter-institutional coordination, enhancement of human resource capacity, and the establishment of progressive yet balanced regulations that respect civil rights. By

comprehensively strengthening ideological and digital resilience, Indonesia can preserve its sovereignty and national stability amid the escalating dynamics of global asymmetric warfare.

Keywords: Warfare, Ideology, Asymmetric, Digital, Cyber

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi di era Revolusi Industri 4.0 telah membawa dampak signifikan terhadap dinamika keamanan nasional.¹ Negara-negara tidak lagi hanya menghadapi ancaman dalam bentuk konvensional seperti invasi militer, namun juga harus bersiap menghadapi bentuk-bentuk baru perang yang bersifat asimetris. Perang asimetris (*asymmetric warfare*) merupakan konflik yang tidak seimbang antara dua pihak, di mana satu pihak menggunakan strategi non-konvensional untuk mengalahkan pihak yang lebih kuat secara militer, ekonomi, atau teknologi.² Dalam konteks ketahanan nasional, perang asimetris memiliki karakteristik yang kompleks karena menyasar aspek-aspek non-militer seperti ideologi, informasi, psikologi, ekonomi, hingga politik.

Perang asimetris telah menjadi paradigma ancaman kontemporer yang menggeser konvensi peperangan tradisional. Berbeda dengan perang simetris yang mengandalkan kekuatan militer seimbang, perang asimetris dicirikan oleh ketimpangan sumber daya, strategi nirmiliter, dan eksploitasi kerentanan multidimensi terutama melalui serangan pemikiran (*cognitive warfare*) dan digital. Indonesia, sebagai negara dengan populasi terbesar keempat dunia dan kekayaan sumber daya alam melimpah, menjadi target utama perang model ini.

Perang asimetris sering kali berlangsung dalam ruang siber (*cyber space*) dan ranah kognitif (*cognitive domain*), di mana senjata utama bukan lagi peluru dan bom, melainkan manipulasi informasi, penyebaran hoaks, propaganda, dan serangan digital (*cyber attack*) yang menyasar infrastruktur kritical nasional, sistem pemerintahan, serta pola pikir masyarakat. Keberadaan media sosial, big data, dan kecerdasan buatan telah menjadi alat yang ampuh dalam mendistorsi persepsi publik, menggoyahkan kepercayaan terhadap institusi negara, serta mengadu domba antar elemen bangsa.

Dalam konteks Indonesia, tantangan ketahanan nasional semakin kompleks. Sebagai negara demokrasi terbesar ketiga di dunia dengan jumlah penduduk yang sangat besar dan keberagaman budaya, suku, serta agama, Indonesia rentan terhadap eksploitasi oleh aktor-aktor asing maupun domestik yang memiliki kepentingan untuk menciptakan instabilitas sosial-politik. Fenomena *post-truth* dan *echo chamber* di ruang digital menciptakan polarisasi opini, memperkuat sentimen primordial, serta melemahkan

¹ Anita Asnawi, "Kesiapan Indonesia Membangun Ekonomi Digital Di Era Revolusi Industri 4.0," *Syntax Literate ; Jurnal Ilmiah Indonesia* 7, no. 1 (2022), <https://doi.org/10.36418/syntax-literate.v7i1.5739>.

² Azis Rahmani, "Network Centric Warfare Dan Perang Asimetris Di Afghanistan," *Jurnal Keamanan Nasional* 4, no. 2 (2018), <https://doi.org/10.31599/jkn.v4i2.400>.

semangat persatuan dan nasionalisme.³ Mantan Menteri Pertahanan Jenderal TNI (Purn.) Ryamizard Ryacudu bahkan menyatakan bahwa dampak perang asimetris "lebih dahsyat daripada bom atom" karena kemampuannya melumpuhkan sendi-sendi ideologi, politik, ekonomi, sosial, dan budaya (Astagatra) secara sistematis.⁴

Berdasarkan Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, pertahanan negara adalah segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia (NKRI), dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara.⁵ Dalam definisi ini, pertahanan tidak semata-mata dipahami sebagai urusan militer, tetapi merupakan tanggung jawab bersama seluruh komponen bangsa. Dalam hal ini, ancaman non-militer seperti perang informasi dan serangan digital merupakan bagian integral dari tantangan pertahanan yang harus diantisipasi.

Ketahanan bangsa, menurut konsep dalam Keputusan Presiden RI Nomor 28 Tahun 2008 tentang Kebijakan Umum Ketahanan Nasional, merupakan kondisi dinamis bangsa dalam menghadapi dan mengatasi berbagai tantangan, ancaman, gangguan, dan hambatan yang dapat mengancam eksistensi dan kedaulatan negara. Ketahanan ini meliputi berbagai aspek: ideologi, politik, ekonomi, sosial budaya, pertahanan dan keamanan, serta teknologi informasi.⁶ Dengan demikian, perang asimetris yang mengancam pemikiran dan dilakukan melalui serangan digital menjadi isu krusial dalam kerangka ketahanan bangsa. Selanjutnya berbagai regulasi nasional seperti UU Nomor 1 Tahun 2022 tentang Hubungan Kekuatan Nasional,⁷ Peraturan Menkominfo Nomor 29 Tahun 2010 tentang Pengamanan Jaringan Internet, dan Pedoman Pertahanan Siber Kemhan diterbitkan yang pada intinya untuk mengantisipasi berbagai pelanggaran hukum yang muncul mengingat semakin kompleksnya ancaman yang terus berkembang di Indonesia.

Lebih jauh lagi, konsep *soft power* yang diperkenalkan oleh Joseph S. Nye Jr. memberikan pemahaman bahwa kekuatan suatu negara tidak hanya dilihat dari aspek militer dan ekonomi (*hard power*), tetapi juga dari kemampuan untuk memengaruhi pihak lain melalui daya tarik budaya, nilai-nilai politik, dan kebijakan luar negeri.⁸ Dalam konteks

³ A G Eka Wenats Wuryanta, "Post-Truth, Cyber Identity Dan Defisit Demokrasi," 2018, <https://doi.org/10.31219/osf.io/up96m>.

⁴ Erman Anom, "Pemahaman Ketahanan Nasional Dalam Upaya Memperkokoh Keutuhan NKRI," *Forum Ilmiah Indonusa* 5, no. 03 (2008).

⁵ Kris Wijoyo Soepandji and Muhammad Farid, "Konsep Bela Negara Dalam Perspektif Ketahanan Nasional," *Jurnal Hukum & Pembangunan* 48, no. 3 (2018), <https://doi.org/10.21143/jhp.vol48.no3.1741>.

⁶ Fahmi Irahmsyah, "Sustainable Development Goals (SDGs) Dan Dampaknya Bagi Ketahanan Nasional," *Jurnal Lemhannas RI* 7, no. 2 (2020), <https://doi.org/10.55960/jlri.v7i2.71>.

⁷ Undang-Undang Indonesia, "UU Nomor 1 Tahun 2022 Tentang HKPD," *Lembaran Negara Republik Indonesia Nomor 6757*, no. 104172 (2022).

⁸ Joseph S Nye, "Soft Power Joseph S. Nye, Jr. Foreign Policy, No. 80, Twentieth Anniversary (Autumn, 1990), 153-171," *Foreign Policy*, no. 80 (2006).

perang asimetris, aktor-aktor negara maupun non-negara dapat menggunakan strategi *soft power* untuk memengaruhi opini publik, menggerus legitimasi pemerintah, serta mengganggu stabilitas dalam negeri negara target.

Strategi *hybrid warfare* yang menggabungkan unsur militer dan non-militer, fisik dan digital, legal dan ilegal, semakin memperkuat ancaman terhadap ketahanan nasional. Aktor-aktor seperti kelompok terorisme, jaringan intelijen asing, hingga korporasi multinasional dapat memanfaatkan kerentanan sistem digital suatu negara untuk melumpuhkan fungsi-fungsi vital negara, mencuri data penting, atau memanipulasi hasil pemilu. Di Indonesia, serangan siber terhadap situs resmi pemerintah, kebocoran data pribadi, serta propaganda radikal melalui media sosial menjadi bukti nyata bahwa ketahanan digital dan pemikiran bangsa sedang dalam tekanan serius.

Dalam perspektif hukum, ancaman pemikiran dan serangan digital telah direspon dengan berbagai regulasi nasional seperti UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah beberapa kali direvisi untuk menjawab perkembangan zaman. Selain itu, UU Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme juga memberikan ruang hukum untuk menghadapi ancaman dari kelompok ekstrem yang menggunakan dunia maya sebagai alat perekrutan dan propaganda. Namun demikian, tantangan hukum tetap ada, terutama dalam hal penegakan hukum lintas batas (*extraterritorial jurisdiction*), perlindungan hak-hak sipil dalam penindakan digital, serta keteringgalan regulasi dari kecepatan perkembangan teknologi.

Isu ini juga menyentuh aspek *cyber sovereignty* atau kedaulatan digital.⁹ Dalam era globalisasi, penguasaan terhadap teknologi informasi menjadi syarat mutlak bagi suatu negara untuk mempertahankan kedaulatannya. Negara yang tidak memiliki infrastruktur digital yang kuat dan sistem pertahanan siber yang andal akan menjadi korban dari intervensi asing, pencurian data strategis, dan manipulasi opini publik. Oleh karena itu, pembangunan kapasitas nasional dalam bidang teknologi informasi, literasi digital, dan regulasi siber harus menjadi prioritas utama dalam kebijakan pertahanan nasional.

Lebih dari itu, ketahanan pemikiran bangsa juga berakar pada pendidikan karakter, ideologi Pancasila, dan kesadaran bela negara. Generasi muda harus dibekali dengan nilai-nilai kebangsaan, pemikiran kritis, dan wawasan kebhinekaan agar tidak mudah terpengaruh oleh paham radikal, disinformasi, dan ideologi transnasional. Lembaga pendidikan, tokoh agama, dan media massa memiliki peran sentral dalam membentuk opini publik yang sehat dan memperkuat integritas kebangsaan.

⁹ Khairun Nisa, "Diplomasi Digital Dan Kedaulatan Siber Dalam Hubungan Internasional: Analisis Komparatif Kedaulatan Digital Indonesia Dan Negara Di Amerika Utara (Kanada Dan Meksiko)," *Jurnal Studi Diplomasi Dan Keamanan* 14, no. 1 (2022).

Di tengah situasi global yang semakin tidak menentu, di mana konflik geopolitik dan rivalitas kekuatan besar menimbulkan berbagai *proxy war* dan perang informasi, Indonesia harus mampu memperkuat ketahanan bangsanya secara holistik. Tidak cukup hanya mengandalkan kekuatan militer, tetapi juga perlu membangun ketahanan digital, ketahanan informasi, dan ketahanan ideologis yang tangguh. Dalam hal ini, pendekatan hukum yang progresif, terintegrasi dan antisipatif sangat dibutuhkan agar negara mampu merespon berbagai bentuk ancaman asimetris secara efektif.

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, terdapat urgensi untuk menganalisis bentuk-bentuk baru ancaman terhadap ketahanan bangsa yang tidak lagi bersifat konvensional, melainkan bergerak dalam ranah non-fisik seperti serangan terhadap pemikiran dan melalui sarana digital, maka rumusan masalah yang diajukan adalah; bagaimana strategi hukum dan kebijakan nasional dalam memperkuat ketahanan bangsa menghadapi bentuk-bentuk perang asimetris, khususnya yang menasar pemikiran dan dilakukan melalui serangan digital?.

B. Metode Penelitian

Metode penelitian yang digunakan dalam tulisan ini adalah menggunakan pendekatan normatif-empiris yang menggabungkan analisis terhadap norma hukum dengan pengamatan terhadap fenomena sosial yang relevan.¹⁰ Jenis penelitian ini bersifat deskriptif-analitis, bertujuan untuk menguraikan dan memahami strategi ketahanan bangsa dalam menghadapi perang asimetris, khususnya dalam bentuk serangan digital dan infiltrasi pemikiran. Data diperoleh melalui studi kepustakaan dan dokumentasi atas berbagai literatur, laporan, dan sumber data sekunder yang mendukung kajian. Teknik analisis yang digunakan bersifat kualitatif, dengan menginterpretasikan temuan berdasarkan teori ketahanan nasional, perang asimetris, dan strategi komunikasi. Melalui penelitian ini diharapkan dapat memberikan pemahaman yang komprehensif mengenai hubungan antara kebijakan negara, sistem pertahanan non-militer, dan dinamika sosial yang terjadi di ruang digital dalam kepentingannya menjaga keutuhan negara.

C. Pembahasan

Dalam menghadapi dinamika global yang terus berubah, bangsa Indonesia dihadapkan pada bentuk-bentuk ancaman baru yang tidak lagi bersifat konvensional. Perang tidak lagi selalu dimaknai sebagai konflik bersenjata terbuka antar negara, melainkan juga sebagai pertarungan di ranah non-fisik yang bersifat tersembunyi, tidak terduga, dan berdampak luas. Salah satu bentuk dari evolusi konflik tersebut adalah perang asimetris, yakni jenis peperangan yang dilakukan secara tidak seimbang oleh aktor-aktor yang tidak setara kekuatan atau metode. Perang asimetris sering kali

¹⁰ Fuad and Rio Rama Baskara, "Managing State Finances Amid Globalization; Challenges And Opportunities," *Widya Pranata Hukum : Jurnal Kajian Dan Penelitian Hukum* 6, no. 1 (November 19, 2024): 118–32, <https://doi.org/10.37631/widyapranata.v6i1.1578>.

memanfaatkan celah ideologi, celah regulasi, serta ruang digital sebagai medan utama pertarungan, menjadikannya tantangan nyata bagi ketahanan suatu bangsa.

Dalam konteks Indonesia, kondisi ini menjadi semakin krusial mengingat keberagaman masyarakat, luasnya wilayah, serta tingginya penetrasi teknologi digital di semua lapisan kehidupan. Ketahanan bangsa tidak hanya ditentukan oleh kekuatan militer, tetapi juga oleh sejauh mana masyarakat dan institusi negara mampu menghadapi serangan terhadap pemikiran, opini, dan informasi yang dapat melemahkan integritas nasional. Oleh karena itu, pada bagian pembahasan berikut, akan mengelaborasi dimensi ancaman asimetris secara menyeluruh, strategi nasional dalam menangulangnya, hingga upaya memperkuat ketahanan ideologis dan sistem kelembagaan negara di tengah era disrupsi informasi. Berikut penjabarannya:

1. Dimensi Ancaman Asimetris dalam Konteks Ketahanan Bangsa

Perang asimetris telah berkembang menjadi salah satu bentuk ancaman strategis yang semakin kompleks dalam dinamika keamanan global modern karena mampu mengaburkan batas antara kondisi perang dan damai. Berbeda dengan konflik bersenjata konvensional yang menempatkan kekuatan militer sebagai instrumen utama dalam menghadapi musuh secara langsung, perang asimetris menggunakan pendekatan yang tidak seimbang melalui kombinasi strategi politik, ideologi, ekonomi, teknologi, serta operasi informasi. Konflik jenis ini dapat melibatkan aktor negara maupun non-negara, seperti kelompok kepentingan, organisasi transnasional, hingga individu atau komunitas yang memanfaatkan kemajuan teknologi digital. Media sosial, ruang siber, opini publik, dan disinformasi menjadi instrumen strategis yang digunakan untuk memengaruhi cara berpikir masyarakat, membentuk persepsi, serta menciptakan ketidakstabilan tanpa harus menggunakan kekuatan militer secara terbuka. Dalam konteks ketahanan bangsa, perang asimetris menjadi tantangan multidimensional karena mampu menyerang berbagai aspek fundamental negara secara bersamaan, mulai dari ideologi, politik, ekonomi, sosial budaya, hingga sistem informasi nasional.

Ketahanan bangsa pada era modern tidak hanya ditentukan oleh kemampuan pertahanan fisik, tetapi juga oleh kapasitas negara dan masyarakat dalam mengenali, mencegah, serta mengelola berbagai bentuk ancaman nonmiliter. Ancaman pemikiran dan serangan digital menjadi bagian dari strategi sistematis yang bertujuan memengaruhi kesadaran kolektif masyarakat, melemahkan kepercayaan terhadap institusi negara, serta mengikis nilai-nilai kebangsaan. Apabila tidak ditangani secara efektif, ancaman tersebut dapat menciptakan disrupsi sosial yang berkepanjangan dan berpotensi mengganggu stabilitas nasional.

Salah satu bentuk nyata perang asimetris di era digital adalah munculnya radikalisasi daring, ujaran kebencian, polarisasi politik, propaganda, serta penyebaran informasi palsu atau hoaks. Ruang siber memberikan peluang bagi pelaku untuk melakukan pendekatan yang lebih terarah melalui pemanfaatan data pengguna, pola perilaku, dan karakteristik

psikologis masyarakat. Kondisi ini menyebabkan kelompok tertentu, terutama generasi muda dengan tingkat literasi digital yang rendah, menjadi lebih mudah dipengaruhi oleh narasi manipulatif. Oleh karena itu, penguatan ketahanan digital, peningkatan literasi informasi, serta kolaborasi antara pemerintah, masyarakat, dan sektor teknologi menjadi langkah penting dalam menghadapi ancaman perang asimetris yang semakin berkembang.

2. Strategi Nasional dalam Menangkal Serangan Digital

Ketahanan digital menjadi salah satu pilar penting dalam sistem pertahanan nasional kontemporer karena perkembangan teknologi informasi telah mengubah karakter ancaman terhadap keamanan negara. Indonesia, dengan jumlah pengguna internet yang mencapai lebih dari 200 juta pengguna,¹¹ menjadi ruang strategis yang rentan terhadap berbagai bentuk operasi digital, baik yang bermotif ekonomi, politik, maupun ideologis. Tingginya tingkat konektivitas masyarakat memberikan manfaat besar bagi pembangunan nasional, namun di sisi lain juga membuka peluang munculnya ancaman seperti serangan siber, pencurian data, manipulasi informasi, propaganda digital, serta penyebaran disinformasi. Oleh karena itu, negara perlu membangun strategi pertahanan siber yang komprehensif dengan melibatkan kolaborasi antara pemerintah, sektor swasta, akademisi, serta masyarakat sipil sebagai bagian dari ekosistem keamanan digital nasional.

Salah satu strategi utama dalam memperkuat ketahanan digital adalah pembangunan arsitektur keamanan siber nasional yang terintegrasi. Upaya ini mencakup penguatan kelembagaan yang memiliki kewenangan dalam menangani ancaman siber, peningkatan kompetensi sumber daya manusia di bidang keamanan informasi, serta pengembangan infrastruktur teknologi yang mampu menghadapi berbagai bentuk serangan digital. Perlindungan terhadap infrastruktur kritical nasional menjadi prioritas karena gangguan terhadap sektor strategis, seperti layanan publik, sistem pemilu, data kesehatan, perbankan, dan keuangan negara, dapat berdampak langsung terhadap stabilitas nasional.

Selain pendekatan teknis, strategi ketahanan digital juga harus diarahkan pada aspek preventif melalui peningkatan literasi digital masyarakat. Kemampuan masyarakat dalam memahami keamanan informasi, mengenali hoaks, serta menyaring konten digital menjadi benteng awal dalam menghadapi ancaman perang informasi. Pendidikan literasi media dan penguatan nilai-nilai ideologi nasional perlu diintegrasikan dalam kurikulum pendidikan sejak tingkat dasar agar generasi muda memiliki kemampuan berpikir kritis dan tidak mudah terpengaruh oleh propaganda maupun narasi ekstrem yang berkembang di ruang digital.

¹¹ Jamalul Izza, "Pengguna Internet Indonesia Hampir Tembus 200 Juta Di 2019 – Q2 2020," *Asosiasi Penyelenggara Jasa Internet Indonesia*, 2020.

3. Ketahanan Ideologis dan Perang Pemikiran

Ketahanan ideologi merupakan salah satu komponen fundamental dalam menjaga keberlangsungan dan keutuhan bangsa di tengah perkembangan ancaman nonmiliter yang semakin kompleks. Dalam konteks perang asimetris, ideologi Pancasila menjadi salah satu aspek strategis yang berpotensi menjadi sasaran pelemahan oleh aktor-aktor tertentu yang memiliki kepentingan ideologis, politik, maupun ekonomi. Berbeda dengan serangan konvensional yang dilakukan secara terbuka, serangan terhadap ideologi bangsa umumnya berlangsung secara tidak langsung, sistematis, dan bersifat persuasif. Upaya tersebut dapat muncul melalui berbagai saluran, seperti media sosial, industri hiburan, ruang diskusi publik, hingga konten keagamaan yang telah mengalami distorsi makna untuk memengaruhi pola pikir masyarakat.

Perang pemikiran dalam ruang digital dilakukan melalui penyebaran narasi yang bertentangan dengan nilai-nilai kebangsaan, seperti upaya mempertentangkan agama dengan negara, mereduksi legitimasi simbol-simbol nasional, serta menyebarkan ketidakpercayaan terhadap pemerintah melalui informasi yang tidak berdasarkan fakta. Strategi ini bertujuan membangun persepsi negatif secara perlahan dan menciptakan disonansi kognitif dalam masyarakat, yaitu kondisi ketika terjadi ketidaksesuaian antara pemahaman, sikap, dan tindakan warga negara terhadap nilai serta identitas nasionalnya. Jika dibiarkan, kondisi tersebut dapat melemahkan rasa persatuan dan solidaritas sosial.

Dalam menghadapi ancaman tersebut, penguatan ketahanan ideologi membutuhkan keterlibatan berbagai elemen bangsa. Institusi pendidikan memiliki peran penting dalam membentuk karakter generasi muda melalui penguatan pendidikan kewarganegaraan dan internalisasi nilai-nilai Pancasila secara kontekstual. Selain itu, tokoh masyarakat dan tokoh agama berperan sebagai penjaga nilai sosial dengan memberikan pemahaman keagamaan yang moderat serta mencegah berkembangnya paham radikal. Media juga harus berperan aktif dalam menghadirkan informasi yang edukatif dan bertanggung jawab guna membangun masyarakat yang kritis terhadap berbagai bentuk propaganda digital.

4. Evaluasi Kebijakan dan Kelembagaan Nasional

. Dalam menghadapi perang asimetris yang semakin kompleks, efektivitas kebijakan dan kelembagaan menjadi salah satu indikator utama dalam mengukur ketahanan institusional suatu negara. Ancaman modern tidak lagi hanya berbentuk serangan fisik terhadap wilayah negara, tetapi juga berkembang melalui ruang digital, manipulasi informasi, serangan siber, serta penyebaran ideologi yang dapat mengganggu stabilitas nasional. Indonesia telah membangun sejumlah instrumen kelembagaan untuk menghadapi tantangan tersebut, di antaranya Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika, serta berbagai satuan tugas yang memiliki fokus

dalam penanganan radikalisme dan terorisme berbasis digital¹². Keberadaan lembaga-lembaga tersebut menunjukkan adanya kesadaran negara terhadap pentingnya penguatan keamanan nasional dalam menghadapi bentuk ancaman yang bersifat multidimensional.

Namun, tantangan utama tidak hanya berkaitan dengan keberadaan institusi, tetapi juga terletak pada efektivitas koordinasi, integrasi kebijakan, dan sinkronisasi kewenangan antar-lembaga. Kompleksitas perang asimetris membutuhkan mekanisme kerja lintas sektor yang cepat, fleksibel, dan adaptif karena ancaman digital dapat berkembang dalam hitungan waktu yang sangat singkat. Berbagai kasus serangan siber, pencurian data, maupun penyebaran narasi ekstrem sering kali menghadapi hambatan dalam penanganannya akibat adanya tumpang tindih kewenangan, perbedaan prioritas antarinstansi, serta prosedur birokrasi yang belum sepenuhnya responsif terhadap karakter ancaman digital.

Di sisi lain, penyusunan kebijakan keamanan digital juga menghadapi dilema antara kebutuhan menjaga stabilitas nasional dengan perlindungan terhadap hak kebebasan berekspresi. Regulasi yang terlalu represif berpotensi membatasi ruang demokrasi dan menimbulkan ketakutan masyarakat dalam menyampaikan pendapat. Oleh karena itu, kebijakan penanganan perang asimetris harus dirancang secara proporsional, berbasis bukti, serta tetap menghormati prinsip hak asasi manusia.

Selain aspek keamanan, evaluasi kebijakan perlu mencakup penguatan diplomasi digital, perlindungan data pribadi, dan pembangunan ekonomi digital yang memiliki daya tahan terhadap intervensi eksternal. Negara perlu mendorong kedaulatan data, pengembangan teknologi nasional, serta peningkatan kapasitas sumber daya manusia agar ekosistem digital Indonesia tidak hanya aman, tetapi juga mandiri dan mampu menghadapi dinamika ancaman global.

5. Rekomendasi Strategis untuk Penguatan Ketahanan Nasional

Berdasarkan analisis di atas, maka diperlukan serangkaian rekomendasi strategis untuk memperkuat ketahanan bangsa dalam menghadapi perang asimetris:

Pertama, diperlukan kebijakan nasional yang menyeluruh mengenai perlindungan ruang digital dan penguatan ketahanan ideologis masyarakat. Hal ini harus tertuang dalam rencana induk pertahanan non-militer yang mengintegrasikan fungsi keamanan siber, pendidikan ideologi, serta pengawasan informasi publik. *Kedua*, pembangunan kapasitas sumber daya manusia menjadi faktor kunci. Pemerintah harus mendukung pelatihan dan pendidikan bidang keamanan siber, intelijen digital, dan analisis wacana. Perlu juga didorong kolaborasi antara universitas, sektor swasta, dan lembaga negara dalam riset-riset strategis tentang ancaman siber dan kognitif.

¹² Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2022," *Badan Siber Dan Sandi Negara*, 2022.

Ketiga, perlunya penguatan kerangka regulasi yang responsif terhadap dinamika digital. Regulasi harus fleksibel, adaptif, namun tetap menjamin perlindungan hak warga negara. Penyusunan peraturan hendaknya melibatkan partisipasi publik agar tidak menimbulkan resistensi sosial. *Keempat*, memperkuat peran masyarakat sipil dan komunitas digital sebagai benteng pertahanan informasi. Edukasi publik harus terus digencarkan dengan pendekatan yang kreatif, termasuk melalui platform media sosial, podcast, dan konten visual yang mudah dipahami, dan *Kelima*, pemerintah harus aktif membangun diplomasi digital untuk mengatasi serangan lintas negara, kerja sama regional dalam penanganan ancaman siber, serta advokasi dalam forum internasional terkait kedaulatan digital dan regulasi global.

Pembahasan ini menunjukkan bahwa ketahanan bangsa tidak bisa dilepaskan dari kemampuan negara dan masyarakatnya dalam memahami serta merespons dinamika perang asimetris yang kian kompleks. Kelemahan dalam satu sektor akan berdampak pada melemahnya sektor lainnya. Oleh karena itu, strategi yang terintegrasi, inklusif, dan berbasis pada nilai-nilai kebangsaan menjadi prasyarat utama bagi kelangsungan dan keutuhan Negara Kesatuan Republik Indonesia.

D. Penutup

Berdasarkan analisis mengenai karakteristik dan dinamika perang asimetris, diperlukan serangkaian rekomendasi strategis yang komprehensif untuk memperkuat ketahanan bangsa dalam menghadapi berbagai bentuk ancaman modern. Perang asimetris tidak hanya berkaitan dengan aspek pertahanan dan keamanan, tetapi juga menyentuh dimensi ideologi, teknologi, sosial, ekonomi, serta psikologis masyarakat. Oleh karena itu, respons negara tidak dapat dilakukan secara parsial, melainkan membutuhkan pendekatan lintas sektor yang melibatkan pemerintah, lembaga pendidikan, sektor industri, komunitas digital, dan masyarakat secara luas.

Pertama, diperlukan kebijakan nasional yang menyeluruh mengenai perlindungan ruang digital dan penguatan ketahanan ideologis masyarakat. Kebijakan tersebut perlu dituangkan dalam suatu rencana induk pertahanan nonmiliter yang mampu mengintegrasikan strategi keamanan siber, pendidikan ideologi, pengelolaan informasi publik, serta mekanisme mitigasi terhadap ancaman berbasis kognitif. Negara tidak cukup hanya berfokus pada penanganan serangan setelah terjadi, tetapi juga harus membangun sistem pencegahan melalui deteksi dini terhadap pola propaganda, disinformasi, dan manipulasi opini publik.

Kedua, pembangunan kapasitas sumber daya manusia menjadi faktor kunci dalam memperkuat ketahanan nasional di era digital. Pemerintah perlu memperluas program pendidikan dan pelatihan dalam bidang keamanan siber, intelijen digital, analisis data, serta pemahaman terhadap perang informasi. Pengembangan sumber daya manusia tersebut harus dilakukan melalui kolaborasi antara perguruan tinggi, sektor swasta,

lembaga pemerintah, dan pusat penelitian untuk menghasilkan inovasi serta kajian strategis mengenai ancaman siber dan perang kognitif.

Ketiga, diperlukan penguatan kerangka regulasi yang mampu mengikuti perkembangan teknologi dan karakter ancaman digital yang terus berubah. Regulasi harus bersifat adaptif, berbasis risiko, serta tetap menjamin perlindungan terhadap hak dan kebebasan warga negara. Proses penyusunan kebijakan juga harus melibatkan partisipasi publik agar tercipta keseimbangan antara kepentingan keamanan nasional dan prinsip demokrasi.

Keempat, penguatan peran masyarakat sipil dan komunitas digital menjadi elemen penting dalam membangun pertahanan informasi nasional. Masyarakat harus diposisikan bukan hanya sebagai pengguna teknologi, tetapi juga sebagai aktor pertahanan digital melalui peningkatan literasi media, kemampuan berpikir kritis, dan kesadaran terhadap keamanan informasi. Program edukasi publik perlu dikembangkan secara kreatif melalui media sosial, podcast, maupun konten visual yang mudah dipahami oleh berbagai kelompok masyarakat. Kelima, pemerintah perlu memperkuat diplomasi digital melalui kerja sama internasional dalam menghadapi ancaman lintas negara. Kerja sama regional dan global diperlukan untuk memperkuat pertukaran informasi, penanganan kejahatan siber, serta membangun norma internasional terkait keamanan ruang digital dan kedaulatan data.

Dengan demikian, ketahanan bangsa tidak dapat dilepaskan dari kemampuan negara dan masyarakat dalam memahami serta merespons perkembangan perang asimetris yang semakin kompleks. Kelemahan pada satu sektor dapat menciptakan kerentanan pada sektor lainnya. Oleh karena itu, strategi yang terintegrasi, inklusif, adaptif, dan berlandaskan nilai-nilai kebangsaan menjadi prasyarat utama dalam menjaga stabilitas nasional serta mempertahankan keutuhan Negara Kesatuan Republik Indonesia di tengah perubahan lingkungan strategis global.

Referensi

- Anom, Erman. "Pemahaman Ketahanan Nasional Dalam Upaya Memperkokoh Keutuhan NKRI." *Forum Ilmiah Indonusa* 5, no. 03 (2008).
- Asnawi, Anita. "Kesiapan Indonesia Membangun Ekonomi Digital Di Era Revolusi Industri 4.0." *Syntax Literate ; Jurnal Ilmiah Indonesia* 7, no. 1 (2022). <https://doi.org/10.36418/syntax-literate.v7i1.5739>.
- Badan Siber dan Sandi Negara. "Lanskap Keamanan Siber Indonesia 2022." *Badan Siber Dan Sandi Negara*, 2022.
- Fuad, and Rio Rama Baskara. "Managing State Finances Amid Globalization; Challenges And Opportunities." *Widya Pranata Hukum : Jurnal Kajian Dan Penelitian Hukum* 6, no. 1

- (November 19, 2024): 118–32. <https://doi.org/10.37631/widyapranata.v6i1.1578>.
- Indonesia, Undang-Undang. "UU Nomor 1 Tahun 2022 Tentang HKPD." *Lembaran Negara Republik Indonesia Nomor 6757*, no. 104172 (2022).
- Irhamisyah, Fahmi. "Sustainable Development Goals (SDGs) Dan Dampaknya Bagi Ketahanan Nasional." *Jurnal Lemhannas RI* 7, no. 2 (2020). <https://doi.org/10.55960/jlri.v7i2.71>.
- Jamalul Izza. "Pengguna Internet Indonesia Hampir Tembus 200 Juta Di 2019 – Q2 2020." *Asosiasi Penyelenggara Jasa Internet Indonesia*, 2020.
- Nisa, Khairun. "Diplomasi Digital Dan Kedaulatan Siber Dalam Hubungan Internasional: Analisis Komparatif Kedaulatan Digital Indonesia Dan Negara Di Amerika Utara (Kanada Dan Meksiko)." *Jurnal Studi Diplomasi Dan Keamanan* 14, no. 1 (2022).
- Nye, Joseph S. "Soft Power Joseph S. Nye, Jr. Foreign Policy, No. 80, Twentieth Anniversary (Autumn, 1990), 153-171." *Foreign Policy*, no. 80 (2006).
- Rahmani, Azis. "Network Centric Warfare Dan Perang Asimetris Di Afghanistan." *Jurnal Keamanan Nasional* 4, no. 2 (2018). <https://doi.org/10.31599/jkn.v4i2.400>.
- Soepandji, Kris Wijoyo, and Muhammad Farid. "Konsep Bela Negara Dalam Perspektif Ketahanan Nasional." *Jurnal Hukum & Pembangunan* 48, no. 3 (2018). <https://doi.org/10.21143/jhp.vol48.no3.1741>.
- Wuryanta, A G Eka Wenats. "Post-Truth, Cyber Identity Dan Defisit Demokrasi," 2018. <https://doi.org/10.31219/osf.io/up96m>.