Madani: Jurnal Ilmiah Multidisiplin
Volume 4, Nomor 5, June 2026, P. 169-176
E-ISSN: 2986-6340
Licenced by CC BY-SA 4.0
DOI: https://doi.org/10.5281/zenodo.20763937

Keamanan Kognitif dan Disinformasi dalam Perang Rusia–Ukraina 2022: Analisis Strategi dan Implikasi Keamanan Nasional

Cognitive Security and Disinformation in the Russia–Ukraine War 2022: An Analysis of Strategies and National Security Implications

Nur Rafa Tsabitah Ruslan
Universitas Hasanuddin

Abstrak

Seperti yang terlihat dari cara perang Rusia–Ukraina diperjuangkan sejak 2022, medan pertempuran militer tidak hanya terbatas pada perbatasan, tetapi juga menjangkau pikiran melalui disinformasi dan operasi psikologis. Makalah ini mengkaji produksi dan penyebaran disinformasi oleh aktor negara atau non-negara untuk membentuk pandangan publik, memecah opini domestik, serta mendelegitimasi lawan secara internasional. Dengan demikian, disinformasi digambarkan dalam era pasca-kebenaran sebagai "alat perang asimetris abad ke-21, yang menggunakan media sosial dan teknologi digital untuk memperkuat narasi yang dikonstruksi." Dalam dunia yang bergantung pada ruang informasi global, di mana kerentanan kognitif dan kemampuan untuk memverifikasi fakta adalah faktor yang menstabilkan keamanan nasional. Politik dan masyarakat. Ini menyajikan kerangka analitis untuk menilai pendekatan keamanan kognitif, serta menyerukan pendidikan di semua tingkatan untuk memperkuat ketahanan informasi sekaligus perancangan program pelatihan literasi digital; ia juga mengusulkan untuk mengidentifikasi fungsi komunikasi strategis dalam arsitektur pertahanan nasional.
Kata kunci: *keamanan kognitif, disinformasi, Perang Rusia–Ukraina 2022, perang informasi, keamanan nasional.*

Abstract

As evidenced by the way the Russia–Ukraine War has been fought since 2022, the military battlefield is no longer confined to physical borders but also extends into the realm of the human mind through disinformation and psychological operations. This paper examines the production and dissemination of disinformation by state and non-state actors to shape public perceptions, divide domestic opinion, and delegitimize opponents on the international stage. In this context, disinformation in the post-truth era is portrayed as "a 21st-century asymmetric warfare tool that utilizes social media and digital technologies to amplify constructed narratives." In a world that depends on the global information space, cognitive vulnerabilities and the ability to verify facts have become critical factors in maintaining national security, political stability, and social cohesion. This paper presents an analytical framework for assessing cognitive security approaches and advocates education at all levels to strengthen information resilience through the design of digital literacy training programs. It also proposes integrating strategic communication functions into the national defense architecture.
Keywords: cognitive security, disinformation, Russia–Ukraine War 2022, information warfare, national security.

PENDAHULUAN

Konflik antara Rusia dan Ukraina, yang dimulai pada Februari 2022, menandai tonggak penting dalam studi tentang peperangan modern, di mana dimensi kognitif dan informasional memainkan peran yang setara dengan komponen militer konvensional. Selain serangan fisik, kedua belah pihak telah secara intensif menggunakan propaganda, disinformasi, dan narasi global untuk membangun legitimasi, memengaruhi opini publik, dan melemahkan dukungan internasional lawan mereka. Fenomena ini menggarisbawahi bahwa perang tidak lagi hanya terjadi di medan perang, tetapi juga dalam ranah persepsi kolektif, sehingga memunculkan konsep keamanan kognitif sebagai bagian integral dari keamanan nasional.

Dalam konteks Rusia Ukraina, disinformasi digunakan sebagai instrumen perang asimetris yang menggabungkan strategi psikologis, teknologi digital, dan operasi lintas batas untuk memengaruhi perilaku sosio-politik di berbagai negara. Rusia, misalnya, telah mengembangkan narasi "operasi militer khusus" dan "denazifikasi" untuk membenarkan invasi mereka, sementara Ukraina membangun narasi

perlawanan rakyat dan pertahanan demokrasi di panggung global. Media sosial, deepfakes, dan kampanye digital mempercepat penyebaran narasi-narasi ini, memungkinkan disinformasi bergerak lebih cepat daripada mekanisme verifikasi dan respons negara tradisional.

Implikasi keamanan nasional dari dinamika ini sangat luas. Disinformasi dapat mengikis kepercayaan publik terhadap institusi, memperparah konflik internal, dan mengganggu koordinasi kebijakan luar negeri dan pertahanan. Studi terbaru mengenai perang Rusia-Ukraina menegaskan bahwa kelemahan dalam ketahanan informasi dan literasi digital membuat negara-negara rentan terhadap serangan kognitif transnasional. Oleh karena itu, artikel ini bertujuan untuk menganalisis keamanan kognitif dan strategi disinformasi dalam Perang Rusia-Ukraina 2022, serta menelaah implikasinya terhadap kebijakan keamanan nasional, khususnya dalam konteks penguatan ketahanan informasi dan arsitektur pertahanan modern.

TINJAUAN PUSTAKA

Peran Kognitif

Perang kognitif merupakan konsep yang terus berkembang dalam bidang akademik dan militer, yang berfokus pada penggunaan kemampuan kognitif manusia serta teknologi untuk memengaruhi, melemahkan, mengganggu, atau mengubah proses pengambilan keputusan manusia. Konsep ini menjadi semakin penting dalam situasi keamanan modern karena pihak lawan berupaya merusak integritas proses politik di negara demokratis dan mencapai tujuan strategis maupun militer melalui strategi terkoordinasi di bidang politik, militer, ekonomi, dan informasi. Akar perang kognitif dapat ditelusuri dari praktik manipulasi dan penipuan pada masa awal politik serta peperangan, sebagaimana tercermin dalam strategi klasik Sun Tzu. Seiring perkembangan teknologi informasi, strategi tersebut tidak lagi hanya menargetkan para pengambil keputusan, tetapi juga masyarakat luas melalui propaganda, operasi psikologis, dan pemanfaatan ruang siber. Dalam perkembangannya saat ini, perang kognitif melibatkan penerapan ilmu saraf, ilmu perilaku, dan teknologi digital secara strategis untuk memengaruhi pola pikir dan proses kognitif manusia, sehingga menjadi bagian penting dalam konflik modern dan persaingan strategis global.

Perang kognitif merupakan strategi multifaset yang menargetkan pikiran manusia untuk memengaruhi proses pengambilan keputusan, persepsi, dan struktur sosial (Nikoula & McMahon, 2024). Berbeda dengan perang konvensional yang berfokus pada penghancuran fisik, perang kognitif beroperasi pada ranah ide, emosi, dan keyakinan (Claverie & du Cluzel, 2022). Strategi ini bertujuan memanipulasi fungsi kognitif lawan dengan memperlambat atau mendistorsi proses pengambilan keputusan sehingga menimbulkan kebingungan, demoralisasi, bahkan kehancuran diri. Gangguan terhadap proses tersebut dapat melemahkan kemampuan individu maupun masyarakat dalam merespons krisis dan berbagai tantangan secara efektif (Clarke & Kanke, 2019; Bernal dkk., 2020).

Dalam konteks kontemporer, perang kognitif telah menjadi bagian penting dari strategi yang diterapkan sejumlah negara dengan menggabungkan operasi psikologis tradisional dan teknologi modern, seperti kecerdasan buatan (*artificial intelligence*/AI), media sosial, serta ilmu saraf. Sebagai contoh, kampanye disinformasi Rusia pada pemilihan presiden Amerika Serikat tahun 2016 digunakan untuk menumbuhkan perpecahan dan ketidakpercayaan di masyarakat. Sementara itu, Tiongkok memanfaatkan teknologi berbasis AI untuk menyesuaikan propaganda dan memengaruhi persepsi publik secara global (Dahl, 1996; Claverie & du Cluzel, 2022).

Model analitis: Aliran Informasi Palsu, narasi perang hibrida, Operasi Informasi

Dalam bahasa Inggris, istilah propaganda sering kali memiliki konotasi negatif dan cenderung bernuansa merendahkan. Konotasi tersebut berkembang karena faktor historis, terutama dalam tulisan para penulis Amerika pada awal abad ke-20. Akibatnya, propaganda sering dipandang sebagai sesuatu yang bermasalah, khususnya ketika digunakan dalam sistem demokrasi liberal, terlepas dari tujuan yang ingin dicapai. Namun, terdapat jenis propaganda tertentu yang dianggap sangat bermasalah secara moral

maupun politik. Oleh karena itu, Stanley (2015:37) menggunakan istilah penghasutan sebagai label untuk bentuk propaganda yang dinilai tidak masuk akal dan berbahaya tersebut.

AI, deepfakes, and content automation

Kemajuan dalam bidang kecerdasan buatan (AI) telah secara signifikan mengubah lanskap disinformasi dengan memungkinkan produksi, modifikasi, dan penyebaran konten palsu dengan kecepatan tinggi dan biaya rendah. Jika sebelumnya disinformasi bergantung pada tenaga manusia dan rentang waktu yang relatif lama, kini AI memungkinkan pembuatan teks, gambar, audio, dan video secara otomatis dalam skala besar. Dalam konteks keamanan kognitif, pergeseran ini sangat kritis karena ancaman tidak hanya berasal dari isi pesan, tetapi juga dari volume, kecepatan, dan tingkat realisme konten yang disebarkan. Dengan demikian, AI bukan sekadar alat komunikasi, tetapi juga instrumen strategis yang dapat dimanfaatkan untuk memengaruhi persepsi publik, memperkuat propaganda, dan menciptakan kebingungan informasi.

Salah satu bentuk ancaman yang paling menonjol adalah deepfake konten audio-visual yang dimanipulasi menggunakan teknik pembelajaran mesin agar tampak sangat realistis. Deepfake dapat membuat seolah-olah seseorang mengatakan atau melakukan sesuatu yang sebenarnya tidak pernah terjadi. Akibatnya, kepercayaan publik terhadap bukti visual dan audio menjadi semakin rapuh. Dalam konflik politik dan geopolitik, deepfake dapat digunakan untuk mendiskreditkan figur tertentu, memicu kepanikan, atau menciptakan narasi palsu yang meyakinkan. Bahayanya tidak hanya terletak pada kemungkinan bahwa masyarakat akan mempercayai konten palsu, tetapi juga pada munculnya "ketidakpastian epistemik" suatu kondisi di mana masyarakat mulai meragukan semua informasi yang mereka terima.

Otomatisasi konten memperparah masalah ini karena memungkinkan akun bot, sistem generatif, dan perangkat lunak distribusi otomatis untuk menyebarkan pesan secara masif dan berulang-ulang. Dalam praktiknya, otomatisasi memungkinkan kampanye disinformasi berjalan 24 jam sehari tanpa bergantung pada intervensi manusia yang terus-menerus. Pesan yang sama dapat disebarkan melalui berbagai akun, platform, dan format, sehingga tampak organik dan sah. Strategi ini sangat efektif dalam ekosistem media sosial karena algoritma cenderung memperkuat konten yang sedang tren, emosional, dan sering dibagikan. Dengan demikian, konten otomatis tidak hanya memperluas jangkauan disinformasi tetapi juga mempercepat normalisasi narasi palsu di ruang publik.

Dalam konteks keamanan nasional, kombinasi AI, deepfakes, dan otomatisasi konten menciptakan ancaman multidimensi. Di satu sisi, teknologi ini dapat digunakan untuk operasi informasi, perang psikologis, dan pembentukan opini. Di sisi lain, hal ini juga mempersulit verifikasi fakta, penegakan hukum, dan respons kebijakan karena konten palsu dapat diproduksi lebih cepat daripada mekanisme klarifikasi resmi. Oleh karena itu, keamanan kognitif menuntut pendekatan baru yang tidak hanya berfokus pada pendeteksian konten palsu, tetapi juga pada peningkatan literasi digital, penguatan lembaga verifikasi, dan pengembangan sistem pendeteksian berbasis AI. Dengan kata lain, teknologi yang menciptakan ancaman tersebut juga harus ditangani dengan teknologi, regulasi, dan ketahanan sosial yang memadai.

METODE PENELITIAN

Penelitian ini dirancang dengan menggunakan pendekatan kualitatif karena fokus utamanya terletak pada makna, pemahaman mendalam, dan interpretasi strategi disinformasi dalam konteks perang informasi, bukan pada pengukuran statistik atau pengujian hipotesis kuantitatif. Pendekatan kualitatif dianggap paling sesuai untuk mengurai bagaimana narasi, simbol, dan pesan komunikasi dimobilisasi sebagai instrumen untuk memengaruhi persepsi publik, membentuk realitas sosial, serta berdampak pada keamanan kognitif dan keamanan nasional. Dalam kerangka ini, penelitian ini menggunakan metode studi kasus yang berpusat pada konflik Rusia–Ukraina tahun 2022. Perang Rusia–Ukraina dipilih sebagai studi kasus karena secara jelas menunjukkan bagaimana operasi militer

konvensional berjalan beriringan dengan perang informasi dan kampanye disinformasi sistematis di berbagai saluran media, sehingga memberikan contoh konkret bagaimana domain kognitif telah menjadi arena persaingan pengaruh antar negara.

Penelitian ini berfokus pada identifikasi dan analisis strategi disinformasi yang digunakan oleh aktor pro-Rusia selama invasi Ukraina tahun 2022, serta mengkaji implikasi strategi tersebut terhadap keamanan kognitif masyarakat dan keamanan nasional negara-negara yang menjadi sasaran. Fokus ini mencakup pengamatan terhadap pola narasi, mekanisme penyebaran, dan taktik operasional disinformasi—seperti pengulangan pesan tertentu, penanaman keraguan terhadap sumber informasi resmi, serta produksi narasi yang bertentangan untuk menciptakan kebingungan epistemologis di kalangan masyarakat. Di sisi lain, studi ini juga berupaya memahami bagaimana disinformasi semacam itu dapat mengikis kepercayaan publik terhadap lembaga-lembaga negara, memperparah polarisasi sosial dan politik, serta memengaruhi kemampuan negara dalam merumuskan dan menerapkan kebijakan keamanan nasional. Oleh karena itu, unit analisis dalam studi ini terdiri dari teks dan dokumen, seperti artikel media, pernyataan resmi, dan laporan kebijakan, yang mewakili praktik disinformasi dan respons keamanan nasional seputar invasi tahun 2022.

HASIL DAN PEMBAHASAN

Gambaran Umum Temuan

hasil penelitian mengenai strategi disinformasi dalam perang Rusia–Ukraina tahun 2022 sebagai bentuk ancaman terhadap keamanan kognitif serta dampaknya terhadap keamanan nasional. Hasil penelitian menunjukkan bahwa disinformasi yang menyertai invasi Rusia bukan sekadar aktivitas komunikasi biasa, melainkan bagian dari strategi perang informasi yang dirancang secara sistematis. Operasi militer yang berlangsung di medan perang berjalan bersamaan dengan operasi informasi yang menargetkan persepsi, opini, dan sikap masyarakat. Sasaran utamanya tidak hanya masyarakat Rusia dan Ukraina, tetapi juga publik internasional yang memiliki pengaruh terhadap dinamika konflik. Dalam kondisi tersebut, ruang kognitif yang mencakup pola pikir, keyakinan, serta emosi masyarakat menjadi arena strategis yang memiliki peran sama pentingnya dengan ruang fisik dan siber dalam konteks keamanan nasional modern.

Pola Strategi Disinformasi dalam Perang Rusia–Ukraina 2022

1. Volume dan Saturasi Informasi

Temuan penelitian menunjukkan bahwa salah satu strategi utama yang digunakan adalah produksi informasi dalam jumlah besar. Media dan saluran komunikasi yang mendukung Rusia secara konsisten menyebarkan berbagai konten mengenai operasi militer, sejarah konflik, serta narasi yang menggambarkan Ukraina dan negara-negara Barat sebagai ancaman. Intensitas penyebaran informasi tersebut menyebabkan ruang publik dipenuhi oleh pesan-pesan yang mendukung kepentingan Rusia, sementara informasi yang berlawanan menjadi kurang terlihat. Dalam situasi krisis, masyarakat cenderung lebih mudah menerima informasi yang paling sering mereka temui dibandingkan informasi yang telah terverifikasi. Kondisi ini memberikan keuntungan bagi pihak yang mampu mendominasi arus informasi melalui produksi pesan yang masif.

2. Kecepatan Penyebaran dan Pembentukan Jangkar Kognitif

Pola berikutnya terlihat pada tingginya kecepatan distribusi informasi. Berbagai klaim mengenai pergerakan pasukan, dugaan pelanggaran hukum perang, maupun keberhasilan operasi militer disebarkan segera setelah peristiwa terjadi, bahkan sebelum ada proses verifikasi yang memadai. Informasi yang pertama kali diterima masyarakat sering kali menjadi dasar dalam membentuk persepsi awal terhadap suatu peristiwa. Persepsi awal tersebut kemudian berfungsi sebagai jangkar kognitif yang memengaruhi cara masyarakat memahami informasi berikutnya. Akibatnya, ketika klarifikasi atau koreksi fakta muncul, pandangan yang telah terbentuk sebelumnya tidak mudah berubah. Dalam jangka

panjang, derasnya arus informasi yang cepat dan terus berubah dapat menimbulkan kelelahan kognitif serta menurunkan minat masyarakat untuk melakukan verifikasi terhadap kebenaran informasi.

3. Multiplikasi Kanal dan Ilusi Konsensus

Penelitian juga menemukan bahwa penyebaran disinformasi dilakukan melalui berbagai saluran komunikasi secara bersamaan. Media daring, televisi, platform berbagi video, media sosial, aplikasi pesan instan, hingga jaringan akun anonim dan bot dimanfaatkan untuk memperluas jangkauan pesan. Penggunaan banyak kanal secara simultan menciptakan kesan bahwa suatu narasi didukung oleh berbagai sumber yang berbeda, meskipun sebenarnya berasal dari jaringan yang saling terhubung. Selain itu, pesan disesuaikan dengan bahasa dan karakteristik audiens di berbagai wilayah sehingga lebih mudah diterima. Strategi ini memungkinkan disinformasi menjangkau masyarakat Rusia, Ukraina, negara-negara Barat, serta komunitas internasional yang berperan dalam pembentukan opini global mengenai konflik.

4. Pengabaian Kebenaran Objektif dan Narasi yang Berubah-ubah

Karakteristik lain yang ditemukan adalah minimnya perhatian terhadap konsistensi fakta. Narasi yang disebarkan lebih berorientasi pada pencapaian tujuan politik dan psikologis daripada akurasi informasi. Ukraina sering digambarkan sebagai pihak yang dipengaruhi sepenuhnya oleh Barat, sementara tindakan militer Rusia dipresentasikan sebagai langkah defensif yang diperlukan. Berbagai klaim didukung oleh sumber anonim, pendapat ahli yang tidak jelas identitasnya, video yang dipotong dari konteks aslinya, atau data yang belum diverifikasi. Ketika suatu narasi mulai diragukan kebenarannya, strategi yang digunakan bukan menarik kembali klaim tersebut, melainkan menggantinya dengan narasi baru. Akibatnya, masyarakat menghadapi situasi yang membingungkan karena sulit menentukan informasi mana yang dapat dipercaya.

Dampak Disinformasi terhadap Keamanan Kognitif

1. Kebingungan Informasi dan Kelelahan Kognitif

Dari perspektif keamanan kognitif, berbagai pola disinformasi tersebut menimbulkan kebingungan dan ketidakpastian yang berkepanjangan. Banyaknya informasi yang saling bertentangan serta sulitnya proses verifikasi membuat masyarakat kehilangan kepastian mengenai realitas yang sedang terjadi. Situasi ini dapat memunculkan kelelahan kognitif, sikap sinis, bahkan ketidakpercayaan terhadap seluruh sumber informasi. Dalam kondisi demikian, individu cenderung mempercayai informasi yang sesuai dengan keyakinan atau identitas kelompoknya daripada yang didasarkan pada bukti. Akibatnya, kemampuan masyarakat untuk melakukan penilaian secara rasional dan kritis menjadi semakin lemah.

2. Menurunnya Kepercayaan terhadap Institusi

Disinformasi juga diarahkan untuk melemahkan kepercayaan masyarakat terhadap institusi penting seperti pemerintah, militer, organisasi internasional, dan media arus utama. Berbagai narasi yang menggambarkan institusi tersebut sebagai pihak yang korup, tidak kompeten, atau berada di bawah pengaruh aktor tertentu bertujuan mengurangi legitimasi mereka di mata publik. Kondisi ini menjadi masalah serius karena keberhasilan pemerintah dalam menghadapi krisis sangat bergantung pada tingkat kepercayaan masyarakat. Apabila kepercayaan tersebut menurun, pelaksanaan kebijakan, termasuk kebijakan di bidang pertahanan dan keamanan, akan menghadapi hambatan yang lebih besar.

3. Polarisasi Sosial dan Penguatan Sikap Ekstrem

Hasil penelitian juga menunjukkan bahwa disinformasi sering dikemas dalam bentuk konflik identitas, seperti pertentangan antara Barat dan Rusia, tradisi dan modernitas, atau nasionalisme dan globalisme. Narasi semacam ini mampu membangkitkan emosi yang kuat dan memperdalam perbedaan pandangan di tengah masyarakat. Di media sosial, konten yang memicu kemarahan atau kontroversi biasanya memperoleh tingkat interaksi yang tinggi sehingga lebih sering ditampilkan oleh algoritma. Akibatnya, terbentuk kelompok-kelompok yang hanya terpapar informasi sejalan dengan pandangan

mereka sendiri. Kondisi ini memperkuat polarisasi dan meningkatkan kerentanan masyarakat terhadap berbagai bentuk manipulasi informasi.

Implikasi terhadap Keamanan Nasional

1. Disinformasi sebagai Ancaman Nonmiliter

Penelitian ini menunjukkan bahwa disinformasi perlu dipahami sebagai bentuk ancaman nonmiliter yang memiliki dampak strategis terhadap keamanan nasional. Kampanye disinformasi yang dilakukan secara terorganisasi dapat mengurangi solidaritas sosial, mengganggu proses pengambilan keputusan politik, serta menurunkan legitimasi pemerintah. Dalam situasi konflik, penyebaran narasi yang menonjolkan kelemahan militer atau perpecahan politik dapat mengurangi dukungan masyarakat terhadap kebijakan pertahanan dan menciptakan kondisi yang menguntungkan pihak lawan.

2. Gangguan terhadap Respons Internasional

Selain berdampak pada tingkat domestik, disinformasi juga berpengaruh terhadap respons internasional. Berbagai narasi digunakan untuk mengaburkan fakta mengenai pelanggaran hukum humaniter atau menuduh pihak lain tanpa bukti yang kuat. Banyaknya informasi yang saling bertentangan membuat organisasi internasional maupun kelompok negara kesulitan membangun kesepahaman mengenai langkah yang harus diambil. Akibatnya, proses diplomasi, pemberian sanksi, maupun bentuk respons kolektif lainnya menjadi kurang efektif.

Respons Kebijakan dan Tantangannya

1. Penguatan Pertahanan Informasi dan Literasi Digital

Sebagai bentuk respons terhadap ancaman tersebut, berbagai negara dan organisasi internasional mulai mengembangkan kebijakan yang menempatkan disinformasi sebagai isu keamanan nasional. Langkah yang dilakukan meliputi pembentukan unit komunikasi strategis, penguatan sistem pemantauan informasi, serta peningkatan kerja sama internasional dalam berbagi data dan pengalaman. Selain itu, program literasi media dan literasi digital juga diperluas untuk meningkatkan kemampuan masyarakat dalam mengenali manipulasi informasi, mengevaluasi sumber berita, dan mengendalikan respons emosional terhadap konten yang provokatif. Upaya tersebut bertujuan memperkuat ketahanan kognitif masyarakat agar tidak mudah terpengaruh oleh kampanye disinformasi.

2. Dilema antara Keamanan dan Kebebasan Sipil

Meskipun demikian, penanganan disinformasi menghadirkan tantangan tersendiri. Negara memiliki kewajiban untuk melindungi masyarakat dari dampak informasi yang menyesatkan, tetapi tindakan yang terlalu ketat berpotensi membatasi kebebasan berekspresi dan kebebasan pers. Penggunaan istilah disinformasi secara berlebihan terhadap kritik atau pendapat yang berbeda dapat menimbulkan ketidakpercayaan publik dan membuka peluang penyalahgunaan kewenangan. Oleh karena itu, kebijakan keamanan informasi perlu disusun dengan tetap memperhatikan prinsip transparansi, akuntabilitas, serta mekanisme pengawasan yang jelas agar perlindungan terhadap keamanan nasional tidak mengorbankan hak-hak sipil masyarakat.

Sintesis Hasil dan Implikasi Konseptual

Secara keseluruhan, penelitian ini menunjukkan bahwa strategi disinformasi dalam perang Rusia–Ukraina 2022 dijalankan melalui kombinasi produksi informasi dalam jumlah besar, penyebaran yang cepat, penggunaan berbagai saluran komunikasi, serta fleksibilitas narasi yang tidak selalu berorientasi pada kebenaran faktual. Kombinasi tersebut memberikan dampak langsung terhadap keamanan kognitif masyarakat melalui meningkatnya kebingungan informasi, menurunnya kepercayaan terhadap institusi, dan semakin tajamnya polarisasi sosial. Dampak-dampak tersebut pada akhirnya memengaruhi keamanan nasional karena menghambat kemampuan negara dalam menjaga stabilitas dan merespons ancaman secara efektif. Temuan ini memperkuat pandangan bahwa perlindungan ruang kognitif perlu menjadi bagian penting dalam konsep keamanan nasional, sejajar dengan pertahanan militer dan keamanan siber. Oleh karena itu, diperlukan pendekatan yang

mengintegrasikan aspek teknologi, regulasi, pendidikan, dan budaya untuk membangun ketahanan masyarakat dalam menghadapi perkembangan perang informasi di era digital.

SIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa disinformasi dalam perang Rusia–Ukraina tahun 2022 menjadi bagian penting dari strategi perang informasi yang berjalan bersamaan dengan operasi militer. Disinformasi digunakan tidak hanya untuk membentuk opini publik dan membenarkan tindakan militer, tetapi juga untuk menciptakan kebingungan mengenai fakta yang sebenarnya terjadi. Akibatnya, persepsi, emosi, dan keyakinan masyarakat menjadi sasaran utama dalam upaya mencapai tujuan politik dan militer.

Penelitian ini menunjukkan bahwa strategi disinformasi yang digunakan memiliki ciri-ciri penyebaran informasi dalam jumlah besar, dilakukan dengan cepat, memanfaatkan berbagai media secara bersamaan, serta tidak selalu memperhatikan kebenaran informasi. Berbagai narasi yang saling bertentangan, penggunaan sumber yang tidak jelas, dan penyebaran informasi yang sulit diverifikasi menyebabkan masyarakat kesulitan membedakan informasi yang benar dan yang menyesatkan. Kondisi tersebut membuat opini publik lebih mudah dipengaruhi sesuai kepentingan pihak tertentu.

Dari sudut pandang keamanan kognitif, disinformasi menimbulkan beberapa dampak utama, yaitu kebingungan informasi, kelelahan dalam menyaring informasi, menurunnya kepercayaan terhadap pemerintah dan lembaga internasional, serta meningkatnya polarisasi sosial. Paparan informasi yang terus-menerus dan saling bertentangan membuat masyarakat cenderung mempercayai informasi yang sesuai dengan pandangan atau kelompoknya sendiri. Akibatnya, kemampuan masyarakat untuk berpikir kritis dan mengambil keputusan secara rasional menjadi berkurang.

Dalam konteks keamanan nasional, disinformasi dapat dianggap sebagai ancaman nonmiliter yang serius. Kampanye disinformasi yang dilakukan secara terorganisasi dapat melemahkan persatuan masyarakat, mengganggu proses pengambilan keputusan politik, mengurangi dukungan terhadap kebijakan pemerintah, serta menyulitkan terbentuknya kerja sama internasional. Oleh karena itu, keamanan nasional tidak hanya perlu berfokus pada aspek militer dan siber, tetapi juga pada perlindungan ruang kognitif masyarakat dari berbagai bentuk manipulasi informasi.

SARAN

Berdasarkan hasil penelitian, terdapat beberapa saran yang dapat diberikan.

Pertama, pemerintah dan lembaga keamanan perlu memperkuat sistem pertahanan informasi dengan mengakui disinformasi sebagai ancaman terhadap keamanan nasional. Hal ini dapat dilakukan melalui peningkatan kemampuan pemantauan informasi, analisis kampanye disinformasi, serta penyusunan kontra-narasi yang cepat dan terpercaya. Namun, kebijakan tersebut harus tetap dilaksanakan secara transparan dan akuntabel agar tidak membatasi kritik yang sah dari masyarakat.

Kedua, perlu adanya kerja sama yang lebih erat antara pemerintah, media massa, platform digital, dan organisasi masyarakat sipil dalam menangani penyebaran informasi yang menyesatkan. Kerja sama ini dapat dilakukan melalui penguatan kegiatan pemeriksaan fakta, pelaporan konten manipulatif, serta pertukaran informasi dan pengalaman dalam menghadapi disinformasi.

Ketiga, peningkatan literasi media dan literasi digital perlu menjadi prioritas jangka panjang. Masyarakat perlu dibekali kemampuan untuk memverifikasi informasi, berpikir kritis, memahami cara kerja media digital, serta mengelola respons emosional ketika menerima informasi yang bersifat provokatif. Upaya ini dapat dilakukan melalui pendidikan formal maupun program edukasi di masyarakat.

Keempat, peneliti dan akademisi perlu terus mengembangkan kajian mengenai keamanan kognitif dan perang informasi. Penelitian selanjutnya dapat membahas pengaruh teknologi baru, seperti

kecerdasan buatan dan *deepfake*, serta mengevaluasi efektivitas berbagai kebijakan penanggulangan disinformasi yang telah diterapkan di berbagai negara.

Kelima, pemerintah perlu menjaga keseimbangan antara upaya melawan disinformasi dan perlindungan terhadap kebebasan berekspresi serta kebebasan pers. Kebijakan yang terlalu ketat dapat menimbulkan ketidakpercayaan masyarakat dan berpotensi membatasi ruang demokrasi. Oleh karena itu, setiap kebijakan perlu disusun secara proporsional, transparan, dan melibatkan partisipasi publik.

Selain itu, penelitian ini memiliki keterbatasan karena hanya menggunakan analisis kualitatif terhadap dokumen dan media tertentu dalam periode waktu yang terbatas. Oleh sebab itu, penelitian selanjutnya disarankan menggunakan kombinasi metode kualitatif dan kuantitatif, seperti survei, analisis media sosial, atau eksperimen psikologis. Pendekatan tersebut diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai bentuk, mekanisme, dan dampak disinformasi terhadap keamanan kognitif dan keamanan nasional.

REFERENSI

Aliansi Jurnalis Independen Indonesia, & Zinc Network. (2023, Februari 16). *Hoaks seputar invasi Rusia ke Ukraina membelah persepsi publik di Indonesia*. AJI Indonesia.

Amaritasari, I. (2025). *Keamanan nasional dalam konsep dan standar internasional*. Jurnal Kajian Nasional, 7(1), 1–15. https://ejurnal.ubharajaya.ac.id/index.php/kamnas/issue/download/105/43

Cynthia, K., Setiawan, C. N., & Chandra, S. (2025). Peran media sosial dalam mempengaruhi persepsi publik terhadap perang Rusia–Ukraina. *Nusantara: Jurnal Pendidikan, Seni, Sains dan Sosial Humaniora, 3*(1), 1–10.

Darmawan, A. (2025). Sarana perang pemikiran dalam media digital: Kajian kritis. *Lentera Peradaban: Journal on Islamic Studies, 1*(3), 104–114. https://doi.org/10.61166/lpi.v1i3.17

Fauzan, M., & Rahmawati, L. (2025). Pengaruh literasi digital terhadap ketahanan nasional dalam menghadapi tantangan disinformasi global pada pandemi COVID-19. *Jurnal Ilmiah Nusantara, 3*(1),

Kementerian Pertahanan RI. (2025). *Peran penting aspek kebijakan pertahanan dalam mencapai sistem keamanan nasional*. Pusat Kajian Pertahanan dan Keamanan Nasional. https://www.kemhan.go.id/pothan/wp-content/uploads/2025/02/Peran-Penting-Aspek-Kebijakan-Pertahanan-dalam-Mencapai-Sistem-Keamanan-Nasional.pdf

Kementerian Sekretariat Negara Republik Indonesia. (2025, Juli 6). *Ketahanan informasi dan literasi digital di era cognitive warfare*. Humas Setneg.

Manafe, A., Suryadi, T., & Wibowo, B. (2023). *Perang informasi dan keamanan nasional: Tantangan kebijakan pertahanan Indonesia*. In B. Wibowo et al. (Eds.), *Strategi pertahanan dan keamanan nasional di era teknologi tinggi* (pp. 112–139). Jakarta: Penerbit Pertahanan RI.

Nasution, M. T., & Raudia, A. (2022). *Invasi militer Rusia ke Ukraina pada tahun 2022*. Jurnal Ilmu & Wawasan Perdamaian, 8(1), 1–20. https://jurnal.peneliti.net/index.php/JIWP/article/download/12896/8917

Naufalariq, R. R., Fitri, A., & Surya, M. (2024). *Dinamika strategi pertahanan Rusia melalui perang hibrida (hybrid warfare) dalam konflik dengan Ukraina (2020–2023)*. Dinamika Global Security Journal, 12(2), 45–68.

R. Ramadhan, N., et al. (2023). *Tren penelitian tentang disinformasi dalam konflik Rusia–Ukraina*. Jurnal Kebijakan dan Keamanan Internasional, 10(1), 1–21. https://al-haramjournal.id/index.php/J-CEKI/article/view/15372

Sidratahta, M. (2024). *Keamanan nasional: antara teori dan praktiknya di Indonesia*. Jurnal Strategi dan Pertahanan, 15(2), 33–52.