LEBAH
ISSN 1412-8128 (Print), 2964-9056 (Online) | Volume 18, No. 4 July (2025)
Diterbitkan oleh: Institut Hukum Sumberdaya Alam (IHSA Institute)

Optimasi Sinkronisasi Kebijakan Pertahanan dan Kebijakan Publik terhadap Perang Hibrida demi Kepentingan Nasional

Cecilia F.Harsono[1], Asep Adang Supriyadi[2,] Faonaso Harefa[3], Ignatius Joko Purwanto[4]

[1,2,3,4)] Fakultas Ilmu Pertahanan, Universitas Pertahanan, Jakarta, Indonesia

Article Info

Article history:

Received : Jul 6, 2025
Revised : Jul 20,2025
Accepted : Jul 30, 2025

Keywords :

Integrasi Kebijakan;
Metode Campuran;
Perang Hibrida;
Peran Publik;
Pertahanan Indonesia.

Abstrak

Ancaman perang hibrida yang bersifat dinamis dan multidimensi memadukan instrumen militer dan non-militer seperti disinformasi, perang siber, perang tarif, serta hegemoni negara kuat di berbagai kawasan menuntut integrasi kebijakan pertahanan dan publik secara sistemik dan adaptif di Indonesia. Penelitian ini bertujuan untuk menelaah pengaruh dimensi operasional non-militer terhadap persepsi publik mengenai kesiapan Indonesia dalam menghadapi hybrid warfare, serta merumuskan urgensi strategi sinkronisasi kebijakan guna memperkuat ketahanan nasional. Metode yang digunakan adalah mixed methods, dengan pendekatan kualitatif melalui wawancara dengan pakar dan analisis kebijakan, serta pendekatan kuantitatif menggunakan regresi linear untuk mengukur persepsi publik. Hasil kualitatif menunjukkan pentingnya sinergi lintas kelembagaan pemerintah, penguatan penguasaan teknologi digital, dan tata kelola informasi yang responsif. Temuan kuantitatif mendukung hasil tersebut, dengan nilai determinasi yang sangat tinggi (R^2 = 0,965), menunjukkan bahwa kesiapan nasional Indonesia sangat dipengaruhi oleh efektivitas koordinasi antarlembaga, ketahanan sosial, dan kapasitas pemerintah dalam mengelola disinformasi. Novelty dari penelitian ini terletak pada penggabungan tiga perspektif teoritis Asymmetric Conflict, Security Governance, dan Resilienceke dalam satu kerangka model integrasi kebijakan pertahanan dan publik dalam konteks menghadapi perang hibrida. Penelitian ini memberikan kontribusi terhadap pengembangan literatur mengenai perang hibrida di Indonesia dengan menawarkan model kebijakan berbasis pendekatan whole-of-government dan whole-of-society. Implikasinya, strategi pertahanan masa depan perlu memperkuat adaptasi kelembagaan dan partisipasi publik di seluruh wilayah Indonesia guna meningkatkan resiliensi terhadap ancaman hibrida yang terus berkembang dalam berbagai bentuk.

Abstract

The threat of dynamic and multidimensional hybrid warfare combines military and non-military instruments such as disinformation, cyber war, tariff war, and strong state hegemony in various regions, demanding the integration of defense and public and adaptive defense policies in Indonesia. This study aims to examine the influence of non-military operational dimensions on public perceptions of Indonesia's readiness in dealing with hybrid warfare, as well as formulating the urgency of policy synchronization strategies to strengthen national resilience. The method used is mixed methods, with a qualitative approach through interviews with experts and policy analysis, as well as a quantitative approach using linear regression to measure public perception. Qualitative results show the importance of government institutional cross-agency synergy, strengthening the mastery of digital technology, and responsive information governance. Quantitative findings support these results, with a very high determination value (R^2 = 0.965), showing that Indonesia's national readiness is strongly influenced by the effectiveness of coordination between institutions, social security, and government capacity in managing disinformation. The novelty of this study lies in the combination of three theoretical perspectives Asymmetric Conflict, Security Governance, and Resilience in a framework of defense and public policy integration models in the context of facing hybrid warfare. This study contributed to the development of literature regarding hybrid warfare in Indonesia by offering a policy model based on the whole-of-government approach and whole-office. The implication is that future defense strategies need to strengthen institutional adaptation and public participation in all regions of Indonesia to increase resilience to the threat of hybrids that continue to develop in various forms.

Corresponding Author:

Cecilia F. Harsono,
Prodi Keamanan Nasional
Program Doktoral Pasca Sarjana Universitas Pertahanan

Jalan Salemba Raya No. 14 Jakarta Pusat
cecilia.harsono@doktoral.idu.ac.id

PENDAHULUAN

Dalam menghadapi era ancaman kontemporer yang semakin kompleks, dan multidimensi, strategi keamanan nasional Indonesia memerlukan pendekatan yang lebih adaptif dan holistik. Salah satu respons strategis yang mendesak untuk dikembangkan adalah integrasi menyeluruh antara kebijakan pertahanan dan kebijakan publik dalam satu kerangka nasional yang terpadu (Ullah & Xinlei, 2025). Model integratif ini tidak semata berfungsi untuk menyinergikan fungsi-fungsi kelembagaan antara sektor militer dan sipil, tetapi juga untuk membangun sistem pertahanan yang mampu menjawab dinamika ancaman non-tradisional yang tidak lagi tersegmentasi secara konvensional. Berangkat dari latar belakang perkembangan bentuk ancaman yang paling menonjol dalam arsitektur konflik global dewasa ini adalah *hybrid warfare* dimana konsep *hybrid warfare* merujuk pada metode peperangan modern yang menggabungkan antara instrumen kekuatan militer konvensional dengan serangan non-militer yang bersifat tersembunyi, sistemik, dan berdampak luas (Mumford & Carlucci, 2023).

Dalam kerangka teoretis mengenai ancaman hibrida, dapat dibedakan antara ancaman yang bersifat eksternal dan ancaman yang diperkuat oleh kerentanan internal. Ancaman hibrida eksternal merujuk pada tindakan yang berasal dari aktor negara maupun non-negara asing yang secara langsung menargetkan kedaulatan atau stabilitas suatu negara, seperti serangan siber lintas batas, kampanye disinformasi terkoordinasi, atau tekanan ekonomi dan militer dari luar. Sementara itu, ancaman hibrida yang diperparah oleh kerentanan internal cenderung menunjukkan efektivitas yang lebih tinggi karena memanfaatkan kondisi domestik yang lemah, seperti rendahnya kepercayaan publik terhadap institusi negara, infrastruktur digital yang rentan, atau instabilitas politik dan sosial. Dengan kata lain, meskipun sumber ancamannya dapat serupa, keberhasilan ancaman hibrida sangat bergantung pada sejauh mana kelemahan internal dapat dieksploitasi oleh aktor eksternal.

Serangan dalam bentuk disinformasi, infiltrasi ekonomi, perang siber, pengaruh politik luar negeri, serta operasi psikologis menjadi karakteristik utama dari bentuk peperangan ini. Pola serangan hybrid warfare ini seringkali dirancang untuk menciptakan dislokasi sosial, mengikis legitimasi negara, dan melemahkan kepercayaan publik terhadap institusi formal tanpa harus melibatkan eskalasi militer terbuka. Dalam dua dekade terakhir, ancaman terhadap keamanan nasional telah mengalami transformasi yang sangat signifikan, seiring dengan akselerasi globalisasi dan revolusi teknologi informasi. Fenomena *hybrid warfare* tidak semata menjadi manifestasi evolusi taktik perang modern, tetapi juga mencerminkan dinamika geostrategis kekuatan global. Negara-negara besar seperti Rusia, China, dan Amerika Serikat secara aktif mengembangkan instrumen pengaruh di luar pendekatan militer konvensional, dan mengintegrasikan kekuatan informasi, teknologi, serta tekanan ekonomi sebagai bagian dari strategi proyeksi kekuatan. Dalam konteks ini, *hybrid warfare* digunakan bukan hanya untuk memenangkan pertempuran fisik, tetapi untuk mengendalikan persepsi, memecah kohesi sosial, dan melemahkan struktur negara dari dalam. Kasus Ukraina adalah kombinasi antara operasi militer terselubung, serangan siber, dan disinformasi terstruktur dapat menciptakan instabilitas domestik yang sistemik (Dov Bachmann et al., 2023). Invasi Rusia terhadap Ukraina tidak hanya melibatkan kekuatan tempur di darat, tetapi juga dimensi kognitif yang bertujuan membentuk opini publik, memperlemah legitimasi pemerintah, serta mengguncang ketahanan sosial melalui propaganda digital. Pendekatan serupa, dalam bentuk yang lebih tersembunyi, juga digunakan di kawasan Asia Tenggara, di mana perebutan pengaruh antara China dan Amerika Serikat terjadi secara simultan melalui jalur diplomasi ekonomi, teknologi digital, dan kontrol narasi global (Rogozhina, 2021).

Bagi Indonesia, ancaman hybrid warfare semakin relevan mengingat secara geografis dan geopolitik, Indonesia menempati posisi yang sangat strategis yakni berada di jalur pelayaran global, kaya sumber daya alam, serta berperan sebagai jangkar stabilitas kawasan. Namun, keunggulan ini sekaligus menjadikannya sasaran manuver kekuatan besar, khususnya dalam rivalitas strategis antara Amerika Serikat dan China (Kurniawan et al, 2021). Sengketa Laut China Selatan, dominasi ekonomi China melalui inisiatif Belt and Road, serta pembentukan aliansi AUKUS telah menciptakan lanskap baru di Indo-Pasifik yang berdampak langsung pada kepentingan nasional Indonesia, baik dari aspek pertahanan, kedaulatan wilayah, maupun stabilitas ekonomi (J. J.Driedger, 2021). Di tengah rivalitas

global antara kekuatan besar seperti Amerika Serikat dan China, Indonesia harus mempertahankan keseimbangan hubungan luar negeri tanpa terjebak dalam kutub kepentingan tertentu. Di sisi lain, dominasi investor asing dalam proyek-proyek infrastruktur strategis seperti pelabuhan, energi, dan teknologi informasi menunjukkan bahwa tekanan tidak hanya datang melalui kekuatan militer, tetapi juga melalui instrumen ekonomi dan digital yang tidak terasa namun sistemik (Tritto, 2021). Fenomena ini menggambarkan situasi *hybrid threats* dimana justru yang perlu mendapat perhatian serius adalah bahwa ancaman *hybrid warfare* tidak hanya berasal dari luar, melainkan justru diperkuat oleh kondisi kerentanan internal. Polarisasi politik yang tajam, korupsi struktural, kesenjangan sosial-ekonomi, serta lemahnya literasi digital menciptakan ruang yang lebar bagi aktor eksternal untuk melakukan infiltrasi. Serangan terhadap infrastruktur digital yang vital, penyebaran informasi palsu yang merusak kepercayaan publik, serta pengaruh ekonomi melalui dominasi proyek infrastruktur merupakan bentuk nyata bagaimana ancaman hibrida bekerja secara simultan dan tersembunyi (Sun, L., 2023). Dalam konteks ini, pendekatan keamanan nasional tidak dapat lagi hanya berorientasi pada pembangunan kekuatan militer, melainkan harus dikembangkan melalui strategi yang inklusif, berbasis teknologi, dan mampu memperkuat daya tahan sosial-ekonomi secara menyeluruh.

Adanya sistem *Pertahanan dan Keamanan Rakyat Semesta* (Sishankamrata) yang menjadi basis utama bagi arsitektur pertahanan nasional, menekankan bahwa seluruh komponen bangsa baik militer, sipil, pemerintah, maupun masyarakat memiliki peran kolektif dalam menjaga kedaulatan negara. Namun demikian, tantangan kontemporer menunjukkan bahwa doktrin Sishankamrata menghadapi tekanan yang tidak kecil dari jenis ancaman baru yang tidak kasatmata, seperti infiltrasi digital oleh kekuatan asing, intervensi ekonomi transnasional, serta propaganda lintas batas melalui platform media global (Wigell, 2019). Dalam situasi ini, pertahanan nasional tidak lagi cukup hanya mengandalkan keterlibatan teritorial dalam makna tradisional, tetapi harus diperluas ke dalam ruang digital, ranah kebijakan fiskal, hingga tata kelola informasi publik. Di tengah perubahan tersebut, pendekatan kebijakan pertahanan Indonesia yang selama ini masih bersifat sektoral dan terfragmentasi dinilai tidak lagi memadai untuk menjawab kompleksitas ancaman kontemporer (Neyazi et al., 2022). Bentuk ancaman modern seperti *hybrid warfare* telah mengaburkan batas antara kondisi perang dan damai, antara ranah militer dan sipil, serta antara ancaman internal dan eksternal. Strategi hibrida memungkinkan aktor negara maupun non-negara untuk mengeksploitasi kelemahan struktural dan sistemik suatu bangsa melalui manipulasi opini publik, sabotase infrastruktur digital, disinformasi terstruktur, hingga infiltrasi ekonomi melalui instrumen globalisasi (Mara et al., 2022). Dengan demikian, respons terhadap ancaman tersebut tidak dapat lagi mengandalkan pendekatan sektoral yang parsial, melainkan menuntut reformasi menuju pendekatan lintas sektor dan lintas disiplin.

Lebih jauh, integrasi kebijakan juga mencerminkan respons negara terhadap transformasi karakter konflik global, di mana garis pemisah antara "perang" dan "damai" menjadi semakin kabur (Dragomir, 2023). Ketika aktor negara maupun non-negara dapat melancarkan serangan di ruang siber, memengaruhi opini publik melalui algoritma media sosial, atau melemahkan sektor ekonomi melalui penguasaan jalur distribusi digital, maka ketahanan nasional tidak dapat hanya ditumpukan pada kekuatan militer atau penegakan hukum semata. Dibutuhkan arsitektur kebijakan yang mampu menjembatani antara domain pertahanan dan domain publik dalam satu ekosistem nasional yang tangguh dan responsif.

Dengan demikian, strategi pertahanan nasional ke depan harus diarahkan pada pembangunan sistem yang tidak hanya kuat secara militer, tetapi juga tahan terhadap guncangan informasi, manipulasi sosial, serta intervensi ekonomi yang bersifat laten. Integrasi kebijakan bukan lagi pilihan kebijakan yang bersifat tambahan, melainkan telah menjadi struktur utama dalam desain strategis pertahanan modern. Hal ini menjadi landasan untuk membangun strategi *whole-of-government* dan *whole-of-society* yang mampu melibatkan seluruh komponen bangsa dalam menjaga kedaulatan dan stabilitas nasional secara berkelanjutan. Integrasi antara kebijakan pertahanan dan kebijakan publik menjadi suatu keharusan strategis dalam rangka menjawab tantangan tersebut secara sistemik. Tanpa adanya harmonisasi lintas kebijakan, akan selalu terbuka potensi celah dalam sistem ketahanan nasional yang dapat dieksploitasi oleh aktor hybrid untuk menciptakan instabilitas politik, konflik sosial, dan erosi kepercayaan terhadap institusi negara (Wijnja, 2022).

Lemahnya pengawasan terhadap investasi asing di sektor-sektor strategis dapat membuka ruang infiltrasi ekonomi yang membahayakan kedaulatan nasional. Demikian pula, ketidakterhubungan antara lembaga pertahanan dan kementerian sipil dalam menghadapi serangan siber dapat menyebabkan lambannya respons terhadap krisis digital yang berdampak luas. Menghadapi tantangan

global berupa berkembang pesatnya hybrid warfare sebagai strategi negara-negara besar dan tantangan pelemahan aspek ekonomi, politik, sosial budaya dari dalam negeri maupun pengaruh investor asing membutuhkan reformulasi kebijakan pertahanan yang bersifat inklusif, terintegrasi, dan adaptif terhadap karakteristik ancaman multidimensi. Pemerintah tidak hanya harus menyinergikan peran militer dan sipil, tetapi juga merancang kebijakan yang menggabungkan ketahanan digital, kecakapan informasi publik, perlindungan ekonomi nasional, dan diplomasi strategis sebagai satu kesatuan sistem keamanan nasional. Transformasi sistem pertahanan Indonesia ke depan akan sangat ditentukan oleh kemampuan Indonesia dalam menyatukan fungsi-fungsi kelembagaan lintas sektor menjadi satu arsitektur respons nasional yang tangguh, *agile*, dan kompatibel dengan kompleksitas ancaman hybrid warfare masa kini. Sejalan dengan urgensi tema tersebut, penelitian ini bertujuan untuk menganalisis secara komprehensif bagaimana integrasi antara kebijakan pertahanan dan kebijakan publik dapat diperkuat guna menangkal ancaman hybrid warfare yang semakin kompleks, dinamis dan multidimensi. Melalui pendekatan analisis keamanan nasional, studi ini mengevaluasi sejauh mana dinamika geopolitik global, ketegangan regional di kawasan Indo-Pasifik, serta faktor-faktor domestik seperti ego sektoral, dan lemahnya koordinasi antar-lembaga memengaruhi efektivitas sistem pertahanan Indonesia dalam merespons bentuk ancaman non-konvensional tersebut. Dengan menggunakan kerangka teori *assymmetric conflict* untuk menjelaskan/ menjadi dasar teoritis dalam memahami bentuk ancaman kontemporer dan justifikasi perlunya integrasi kebijakan lintas sektor (Ucko & Marks, 2020) (Krishnan, 2022), dan teori *Security Governance* untuk menjelaskan kenapa *whole-of-government* dan *whole-of-society approach* penting dalam menghadapi *hybrid threats* (Ansell et al., 2023).

Selanjutnya kerangka Teori *Resilience* menjelaskan betapa pentingnya daya tahan sosial, ekonomi, dan digital dalam sistem pertahanan nasional (Soares, 2021), sehingga berdasar ketiga teori tersebut penelitian ini secara khusus menyoroti pentingnya integrasi lintas sektor sebagai landasan dalam membangun ketahanan nasional yang tangguh, tidak hanya dalam dimensi militer, tetapi juga dalam ranah sosial, digital, ekonomi, dan kelembagaan. Evaluasi dilakukan terhadap tingkat kohesi kebijakan lintas sektor serta potensi perumusan model kebijakan strategis yang mampu mendorong respons negara secara adaptif, terkoordinasi, dan berbasis tata kelola yang efektif. Lebih lanjut, dari sisi teoretis, kajian akan ini berkontribusi dalam mengisi kesenjangan literatur mengenai hybrid warfare di Indonesia dan Asia Tenggara dengan menawarkan perspektif integratif berbasis pendekatan keamanan nasional. Sementara itu, secara praktis dan strategis, hasil penelitian ini diharapkan dapat memberikan landasan empirik dan konseptual bagi penyusunan kebijakan nasional yang lebih tanggap terhadap karakter ancaman hibrida, serta mendukung pembangunan arsitektur pertahanan nasional berbasis *whole-of-government* dan *whole-of-society* yang adaptif terhadap lanskap ancaman hybrid warfare secara global.(Genschel, 2022).

METHODS

Penelitian ini menggunakan pendekatan metode campuran (mixed methods) dengan desain eksploratori kuantitatif sekuensial, yang menggabungkan analisis kualitatif berbasis tematik dan analisis kuantitatif deskriptif-inferensial (Pilcher & Cortazzi, 2024). Strategi ini digunakan untuk menggali secara mendalam relasi, dinamika, dan tema-tema utama dalam narasi kebijakan pertahanan dan kebijakan publik, lalu mengkuantifikasinya untuk memahami pola pengaruh dan intensitas hubungan antar konsep dalam konteks hybrid warfare.

Secara khusus, pendekatan kualitatif digunakan untuk mengidentifikasi dan mengkonstruksi tema-tema utama dari narasi diskursus pertahanan dan kebijakan publik melalui teknik analisis isi tematik dengan didukung perangkat lunak NVivo 15, sementara pendekatan kuantitatif digunakan untuk mengkuantifikasi hasil tematik tersebut dalam bentuk frekuensi, korelasi, dan distribusi antar tema atau aktor menggunakan teknik kuantifikasi konten (content metric analysis)(Dhakal, 2022). Hasil kuantifikasi tersebut kemudian diolah secara deskriptif dan inferensial menggunakan perangkat lunak Jamovi untuk mendukung triangulasi bukti dan penguatan interpretasi(Khan, 2022). Pendekatan ini memungkinkan peneliti untuk menggabungkan kedalaman eksplorasi kualitatif dengan kekuatan validasi numerik kuantitatif, serta menyajikan suatu model pemahaman yang utuh terhadap bagaimana integrasi kebijakan pertahanan dan kebijakan publik berkontribusi dalam memperkuat ketahanan nasional terhadap ancaman hybrid warfare.

Teknik pengumpulan data, maka sumber data dalam penelitian ini terdiri dari Data Primer yang dihimpun melalui forum diskusi terfokus (Focus Group Discussion/FGD) yang melibatkan 35

mahasiswa program doktor Ilmu Pertahanan di Universitas Pertahanan Indonesia. Diskusi difokuskan pada persepsi, pengalaman, dan interpretasi peserta terhadap kebijakan integratif dan ancaman hybrid warfare dalam konteks nasional. Adapun data sekunder dikumpulkan dari jurnal-jurnal internasional terindeks Scopus Q1 dan Q2 dalam rentang waktu 2021 – 2025, dokumen-dokumen kebijakan, serta media digital yang relevan dengan isu pertahanan dan hybrid warfare di Indonesia. Termasuk di antaranya analisis pernyataan kebijakan, laporan tahunan Kemenhan, pidato pejabat tinggi, dan laporan think tank global. Teknik pengumpulan data dilakukan melalui pengolahan transkrip hasil diskusi FGD, dan data sekunder untuk dilaksanakan dokumentasi dan pengkodean digital secara sistematis melalui bantuan software NVivo 15, beberapa data yang diperoleh dari website dan media daring lainnya diambil dengan fasilitas NCapture pada NVivo 15 sehingga dapat langsung di coding (Dhakal, 2022).

Teknik analisis data dapat dijabarkan sebagai berikut dimulai dari importasi data ke dalam NVivo 15 berupa transkrip FGD dan dokumen sekunder yang dikumpulkan dari jurnal-jurnal internasional terindeks Scopus Q1 dan Q2 dalam rentang waktu 2021 – 2025, dokumen-dokumen kebijakan, serta media digital yang relevan dengan isu pertahanan dan hybrid warfare di Indonesia. Termasuk di antaranya analisis pernyataan kebijakan, laporan tahunan Kemenhan, pidato pejabat tinggi, dan laporan think tank global. Selanjutnya dilakukan tahapan:

1. Open coding dilakukan untuk mengidentifikasi unit makna awal dari setiap fragmen data(Goyal & Deshwal, 2023).
2. Axial coding digunakan untuk mengelompokkan node tematik ke dalam sub-kategori dan dimensi konseptual (misalnya: integrasi kelembagaan, kebijakan pertahanan, kebijakan publik, dan ancaman hybrid warfare).
3. Query dan visualisasi dijalankan melalui fitur Word Cloud dan Tree Map untuk memetakan intensitas dan keterhubungan antar tema.
4. Matrix coding query digunakan untuk menyusun hubungan antar tema berdasarkan aktor, sektor, dan dimensi isu.
5. Ekspor hasil coding dalam bentuk tabel (matrix query output) untuk tahap kuantifikasi konten.

Teknik analis data berikutnya adalah tahap kuantitatif dengan Teknik Kuantifikasi Konten dan Analisis Statistik (Tütüncü, 2023). Hasil *matrix coding query* yang diolah dalam NVivo dikonversi menjadi data numerik berdasarkan frekuensi keterhubungan antar tema dan aktor. Data ini kemudian diekspor ke Microsoft Excel untuk menjadi dataset yang siap dianalisis menggunakan Jamovi dengan prosedur berikut:

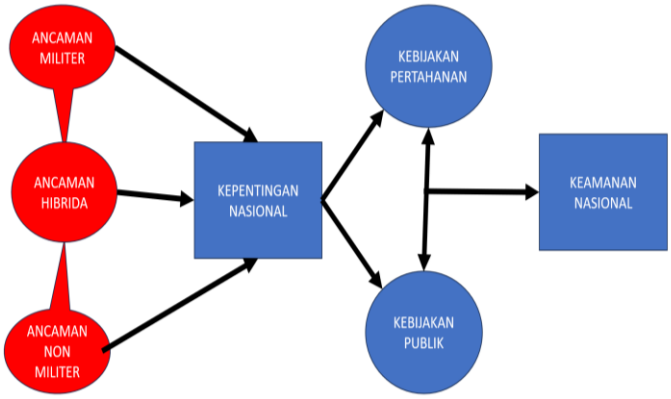
1. Analisis deskriptif dilakukan untuk memetakan persebaran dan dominasi tema.
2. Uji korelasi Pearson digunakan untuk melihat hubungan antar indikator integrasi kebijakan dan indikator ketahanan nasional.
3. Analisis regresi linier sederhana digunakan untuk melihat sejauh mana integrasi kebijakan memengaruhi tingkat ketahanan terhadap hybrid warfare.
4. Visualisasi hasil dilakukan dalam bentuk bar chart dan scatter plot untuk mendukung interpretasi strategis.

Tahapan selanjutnya adalah Validasi sebagai sarana memastikan validitas data yang dilakukan melalui triangulasi sumber data (antara narasi diskusi, dokumen kebijakan, dan konten media). Di dalam NVivo 15 juga dilaksanakan Cross-coding inter-rater untuk menjamin konsistensi penandaan tema dan Comparative cross-tabulation untuk melihat konsistensi pola antara data kualitatif dan numerik(Mitchell-Jones et al., 2025).

Integrasi antara hasil analisis kualitatif berbasis NVivo dan data kuantitatif dapat dipertanggungjawabkan secara metodologis dalam kerangka penelitian mixed methods, khususnya apabila tujuan analisis mencakup identifikasi dan penjelasan hubungan sebab-akibat. Data kuantitatif berfungsi untuk menguji hubungan antarvariabel secara statistik, sedangkan data kualitatif melalui NVivo memberikan pemetaan tematik yang mendalam terkait mekanisme, konteks, dan proses yang mendasari hubungan tersebut. Meskipun pendekatan kualitatif tidak dirancang untuk mengukur kausalitas secara langsung, kontribusinya dapat memperkuat validitas interpretatif terhadap hasil kuantitatif dan memberikan justifikasi empiris yang lebih komprehensif atas konstruksi hubungan kausal dalam suatu fenomena penelitian. Penelitian ini dilaksanakan di Kampus Pascasarjana Program Doktor Ilmu Pertahanan Universitas Pertahan, Matraman Jakarta pada bulan Mei 2025.

HASIL DAN PEMBAHASAN

Hasil dan pembahasan penting untuk mengevaluasi efektivitas sinkronisasi kebijakan pertahanan dan publik dalam menangkal perang hibrida, guna memastikan strategi nasional selaras, adaptif, dan berpihak pada kepentingan nasional, dimana hasil dan pembahasan berikut ini:



Gambar 1. Diagram Kerangka Berpikir

Gambar 1 diatas, merupakan kerangka berpikir gunanya sebagai panduan konseptual peneliti dalam menganalisis bagaimana perang hibrida, yang menggabungkan ancaman militer dan non-militer seperti disinformasi dan serangan siber, sehingga menuntut adanya suatu kebijakan nasional untuk integrasi antara kebijakan pertahanan dan kebijakan publik. Melalui kerangka berpikir ini, dapat digambarkan bagaimana efektivitas koordinasi kelembagaan, penguatan kedaulatan digital, dan partisipasi segenap masyarakat menjadi elemen strategis yang saling berinteraksi untuk memperkuat ketahanan nasional dan menjamin perlindungan kepentingan nasional secara berkelanjutan menuju Indonesia Emas 2045.

Ilustrasi atau Gambaran Perang Hibrida

Gambar 2. Ilustrasi Hybrid Warfare
Sumber: Data Sekunder Website, 2025

Pada gambar 1 diatas, merupakan ilustrasi lanskap konflik kontemporer, *hybrid warfare* yang merepresentasikan bentuk peperangan kompleks dengan mengaburkan batas antara strategi militer konvensional dan taktik non-konvensional(Mumford & Carlucci, 2023). Istilah ini merujuk pada pendekatan gabungan yang melibatkan tindakan terbuka seperti operasi militer reguler, namun juga mencakup metode tersembunyi seperti manipulasi informasi, serangan dunia maya, serta penetrasi ke ranah politik dan ekonomi untuk merusak stabilitas lawan tanpa perlu melibatkan konfrontasi militer skala penuh (Tripodi, 2025). Meningkatnya relevansi strategi ini tidak lepas dari akselerasi teknologi digital dan dinamika globalisasi yang memungkinkan baik aktor negara maupun non-negara mengeksploitasi kerentanan sistem pertahanan dengan metode asimetris (Monaghan, 2019). Salah satu ilustrasi paling menonjol dari penggunaan strategi hibrida adalah krisis Krimea pada tahun 2014, ketika Rusia memanfaatkan propaganda, operasi siber, dan infiltrasi militer tidak resmi untuk menciptakan instabilitas dan menguasai wilayah tanpa pernyataan perang terbuka(Zhang & Zhou, 2023). Fenomena seperti ini sangat menyulitkan bagi doktrin pertahanan tradisional karena karakter serangannya yang tersembunyi, menyebar, dan sulit diprediksi(Dov Bachmann et al., 2023). Oleh karena itu, respons terhadap ancaman semacam ini menuntut pendekatan pertahanan yang tidak hanya berbasis kekuatan militer, tetapi juga mencakup langkah-langkah multidisipliner seperti pembangunan kapasitas kontra-narasi, penguatan sistem pertahanan siber nasional, serta peningkatan koordinasi antarlembaga keamanan dan pemerintahan sipil (Anghel & Džankić, 2023).

Hasil Analisid Data Menggunakan Perangkat Lunak NVivo 15

Gambar 3. Word Cloud Analisis NVivo 15

Visualisasi hasil analisis tematik menggunakan perangkat lunak NVivo menunjukkan peta pemikiran konseptual yang kuat terkait isu *hybrid warfare* dan dinamika kebijakan pertahanan kontemporer. Word Cloud yang dihasilkan memperlihatkan bahwa konsep *security, hybrid threats*, dan *military* menjadi pusat perhatian dalam berbagai dokumen yang dianalisis, yang meliputi publikasi akademik, dokumen kebijakan, dan laporan strategis global. Ketiga istilah tersebut membentuk poros utama yang menjelaskan bagaimana paradigma pertahanan negara telah berevolusi dari struktur militer konvensional menjadi sistem keamanan nasional yang bersifat multidimensi dan adaptif(Kraiwanit et al., 2023). Kemunculan tema "*security*" sebagai elemen yang paling menonjol menegaskan bahwa ancaman kontemporer tidak dapat lagi didekati semata-mata dengan kekuatan bersenjata. Istilah ini, dalam konteks hybrid warfare, mencakup keamanan informasi, keamanan siber, ketahanan sosial, hingga daya tahan ekonomi nasional. Hal ini diperkuat dengan munculnya kata "*cyber*", "*resilience*", dan "*law*", yang menunjukkan bahwa dimensi keamanan kini telah meluas ke ranah digital, regulatif, dan masyarakat sipil. Di sinilah pentingnya pendekatan lintas sektor yang melibatkan berbagai aktor negara, mulai dari militer, badan keamanan siber, hingga lembaga legislatif dan komunitas intelektual (Vogel et al., 2022).

Istilah "hybrid threats" yang menjadi pusat visualisasi merepresentasikan ancaman yang kompleks dan saling terkait. Tidak seperti ancaman konvensional yang bersifat langsung dan terbuka, ancaman hibrida bersifat tersembunyi, terfragmentasi, dan mengandalkan pemanfaatan kerentanan struktural dari dalam sistem negara target. Tema ini juga saling bersinggungan dengan istilah seperti "disinformation", "psychological operations", "economic infiltration", dan "strategic deterrence", yang seluruhnya menggambarkan instrumen non-militer yang digunakan untuk menciptakan ketidakstabilan internal. Fenomena ini mencerminkan kecenderungan meningkatnya ancaman yang bersifat *asymmetric* dan *non-kinetic*, yang sangat sulit dideteksi oleh perangkat pertahanan tradisional (Alam, 2021). Kemunculan kata "military", "forces", dan "defense" tetap menunjukkan bahwa kekuatan bersenjata masih menjadi salah satu komponen penting dalam sistem pertahanan. Namun, posisinya kini bukan sebagai satu-satunya garda terdepan, melainkan menjadi bagian dari arsitektur keamanan yang lebih luas, yang mengintegrasikan aspek hukum (law), kebijakan publik (policy), dan kerja sama internasional (international, NATO). Dalam konteks ini, strategi *whole-of-government* dan *whole-of-society* menjadi sangat relevan, di mana militer bekerja berdampingan dengan lembaga sipil dan masyarakat untuk membangun ketahanan nasional secara menyeluruh (Soares, 2021).

Istilah "government", "political", dan "policy" yang muncul cukup dominan menunjukkan bahwa penanganan hybrid warfare menuntut kesinambungan antar kebijakan lintas sektor dan kepemimpinan strategis dari negara. Ini menjadi penegas bahwa kelemahan dalam koordinasi antar institusi, tumpang tindih regulasi, dan lemahnya literasi digital publik dapat menjadi celah besar yang dimanfaatkan oleh aktor hybrid. Terlebih lagi, kata seperti "state", "order", dan "resilience" memperkuat posisi bahwa sistem pertahanan bukan hanya soal kekuatan menyerang, tetapi juga kemampuan bertahan terhadap tekanan politik, sosial, dan informasi dari dalam maupun luar (Johansen & Martin, 2019). Menarik pula

mencermati kemunculan kata “https”, “doi”, dan “org” dalam visualisasi ini. Kata-kata tersebut secara teknis mungkin mengacu pada metadata rujukan daring, namun secara substansial menunjukkan bahwa medan kontestasi dalam hybrid warfare berlangsung secara intensif di dunia digital dan ekosistem informasi daring. Ini mengindikasikan bahwa kekuatan dan kelemahan dalam mengelola ekosistem digital akan menjadi penentu keberhasilan strategi pertahanan nasional (Dąbrowska et al., 2022).

Kehadiran istilah geopolitik seperti “russian”, “ukraine”, dan “nato” mencerminkan bahwa literatur dan wacana kebijakan tentang hybrid warfare sangat dipengaruhi oleh kasus-kasus nyata seperti aneksasi Krimea dan konflik di Ukraina. Konflik tersebut sering dijadikan studi kasus utama dalam menjelaskan bagaimana aktor negara menggunakan strategi hybrid yang menggabungkan operasi militer tidak resmi, disinformasi, serangan siber, dan tekanan ekonomi dalam rangka menciptakan ketidakstabilan politik dan meraih keuntungan strategis tanpa harus mendeklarasikan perang secara terbuka (Dov Bachmann et al., 2023). Dengan mengacu pada keseluruhan temuan visual tersebut, dapat disimpulkan bahwa narasi pertahanan modern telah bergeser menuju integrasi antara hard power dan soft power, antara alat militer dan alat diplomatik, antara strategi konvensional dan ketahanan sosial. Tantangan hybrid warfare menuntut Indonesia untuk tidak hanya membangun militer yang kuat, tetapi juga memperkuat sistem hukum, infrastruktur digital, literasi informasi masyarakat, dan sinergi kebijakan antara kementerian pertahanan, badan keamanan, serta sektor publik lainnya (Ljungkvist, 2024).

Gambar 4. Tree Map NVivo 15

Visualisasi Tree Map yang dihasilkan melalui NVivo menggambarkan proporsi relatif dari tema-tema yang paling dominan dalam narasi mengenai *hybrid warfare* dan kebijakan pertahanan modern. Setiap kotak dalam visualisasi ini mewakili satu kata kunci atau tema, dengan ukuran kotak yang menunjukkan frekuensi kemunculannya dalam seluruh dataset. Peta visual ini memperkaya hasil Word Cloud sebelumnya dengan struktur hierarki yang lebih sistematis dan memungkinkan analisis kuantitatif awal terhadap *salience* isu dalam dokumen-dokumen yang dianalisis (Chawla et al., 2023). Tema-tema utama yang paling besar dan menonjol dalam Tree Map ini mencakup kata kunci seperti “hybrid”, “warfare”, “military”, “threats”, “security”, “cyber”, “state”, dan “strategic”. Dominasi tema-tema ini menunjukkan bahwa wacana seputar hybrid warfare sebagian besar masih terpusat pada elemen-elemen utama sistem pertahanan negara dalam konteks ancaman multidimensi. Kata "security" dan "military" mendominasi baik secara konseptual maupun statistik, yang mengisyaratkan bahwa meskipun hybrid warfare menekankan metode non-konvensional, narasi utama tetap ditopang oleh keprihatinan akan keamanan nasional dan kesiapsiagaan militer (Joshi, 2023).

Kemunculan tema seperti “cyber”, “disinformation”, “policy”, dan “law” menegaskan pentingnya dimensi non-fisik dalam struktur ancaman hybrid. Ini menunjukkan pergeseran fokus dari sekadar pertempuran militer terbuka ke bentuk penetrasi sistemik yang menyasar ke sektor digital, kelembagaan, dan sosial-politik. Sebagai contoh, frekuensi tinggi kata “cyber” dan “information” menunjukkan bahwa medan konflik kini meluas ke ranah digital dan memerlukan perhatian terhadap keamanan informasi, pertahanan jaringan, serta pengelolaan opini publik (Wall, 2024). Selanjutnya, tema-tema seperti “govern”, “resilience”, “international”, dan “policy” menunjukkan bahwa respons terhadap hybrid warfare menuntut pendekatan lintas sektor dan keterlibatan berbagai aktor negara maupun non-negara. Frekuensi munculnya istilah “nato”, “ukraine”, dan “russian” mengonfirmasi bahwa konflik geopolitik aktual—terutama yang berkaitan dengan Eropa Timur masih menjadi rujukan utama dalam literatur dan praktik pertahanan hibrida. Hal ini dapat dijadikan dasar argumentatif bahwa studi mengenai hybrid warfare di Indonesia harus mengadopsi pendekatan pembelajaran komparatif (*comparative learning*) yang disesuaikan dengan konteks domestik (Libiseller, 2023). Dari sisi *temporal*, kemunculan angka-angka tahun seperti 2016–2022 mengindikasikan bahwa analisis yang digunakan

dalam sumber data relatif terkini, dengan penekanan pada dinamika geopolitik dan inovasi teknologi dalam lima hingga tujuh tahun terakhir. Ini memberi bobot validitas pada argumen bahwa hybrid warfare bukan sekadar konsep, tetapi realitas strategis yang tengah berlangsung dan terus berkembang (Gunneriusson, 2021). Proporsi dan keterhubungan antar tema dalam Tree Map ini menunjukkan bahwa ancaman hybrid warfare memerlukan integrasi menyeluruh antara kebijakan pertahanan, kebijakan publik, sistem hukum, teknologi informasi, serta ketahanan sosial. Data ini menjadi dasar kuat untuk melakukan pemodelan lebih lanjut secara kuantitatif, baik melalui *regresi linier sederhana* berdasarkan frekuensi kemunculan tema, maupun penyusunan indeks ketahanan terhadap hybrid threats berdasarkan kategori isu yang teridentifikasi.

Pengumpulan Data Kuantitatif melalui Kuesioner Persepsi.

Untuk melengkapi analisis kualitatif yang dilakukan melalui NVivo, penelitian ini juga mengintegrasikan pendekatan kuantitatif dengan mengumpulkan data persepsi responden melalui kuesioner terstruktur. Tujuan dari pengumpulan data ini adalah untuk mengukur tingkat persepsi individu terhadap ketahanan nasional dalam menghadapi ancaman hybrid warfare, sehingga dapat dijadikan sebagai variabel dependen (Y) dalam model regresi sengan software Jamovi (Walker et al., 2024). Kuesioner disusun berdasarkan dimensi-dimensi strategis yang relevan dalam konteks pertahanan hibrida, seperti keamanan siber, efektivitas kebijakan publik, koordinasi kelembagaan, literasi informasi, serta persepsi terhadap kesiapan nasional menghadapi ancaman asimetris dan non-konvensional. Instrumen terdiri dari 10 butir pertanyaan yang dinyatakan dalam bentuk pernyataan afirmatif dan diukur menggunakan skala Likert 5 poin (1 = sangat tidak setuju, 5 = sangat setuju). Skala ini dipilih untuk memungkinkan pengukuran derajat kesepakatan responden secara kuantitatif dan analisis statistik lebih lanjut melalui regresi linier (South et al., 2022).

Distribusi kuesioner dilakukan kepada responden yang memiliki latar belakang relevan di bidang pertahanan dan kebijakan publik, yakni mahasiswa Program Doktor Ilmu Pertahanan, analis kebijakan, dan praktisi militer-sipil di lingkungan akademik Universitas Pertahanan Indonesia. Kuesioner disebarkan secara daring menggunakan platform *Google Forms* untuk mempercepat proses pengumpulan dan rekapitulasi data. Setiap responden diminta untuk menjawab seluruh pernyataan berdasarkan persepsi dan pengetahuan pribadi terhadap kesiapan Indonesia dalam menghadapi hybrid warfare. Hasil kuesioner kemudian diolah dalam bentuk skor total persepsi (range 10–50) yang menjadi dasar variabel numerik dalam model regresi linier yang digunakan untuk menguji hubungan antara frekuensi kemunculan tema (hasil NVivo) dan persepsi ketahanan nasional. Berikut adalah tabel pertanyaan tentang persepsi ketahanan nasional sebagai pembentuk variable dependen (Y) yang nantinya akan diolah dengan variabel X (independen/yang mempengaruhi dari hasil Nvivo). Scoring dilakukan dengan skala Likert dimana 1 = Sangat Tidak Setuju, 2 = Tidak Setuju, 3 = Netral, 4 = Setuju, 5 = Sangat Setuju (Tanujaya et al., 2022). Sebagai bagian dari pendekatan kuantitatif dalam penelitian ini, data persepsi dikumpulkan dari 35 panelis (kode A–II) menggunakan instrumen kuesioner dengan 10 indikator yang mencerminkan dimensi utama ketahanan nasional terhadap ancaman hybrid warfare. Instrumen ini menggunakan skala Likert 1–5, dengan skor 1 menunjukkan ketidaksepakatan penuh, dan skor 5 menunjukkan tingkat persetujuan penuh terhadap pernyataan yang diajukan(Christou, 2024). Setiap panelis diminta menilai sepuluh pernyataan yang mencakup topik-topik penting seperti ketahanan siber, kesiapan kelembagaan, peran kebijakan publik, kemampuan negara dalam menjaga kedaulatan digital, hingga efektivitas penanganan disinformasi dan strategi nasional menghadapi ancaman geopolitik.

Hasil Statistik Deskriptif Awal.

Nilai rata-rata keseluruhan dari 35 panelis adalah **3.14**, yang menunjukkan bahwa persepsi terhadap ketahanan nasional Indonesia dalam menghadapi hybrid warfare berada pada tingkat moderat. Dengan kata lain, para panelis memiliki pandangan yang cukup seimbang (tidak pesimistis namun juga tidak sangat optimistis) terhadap kesiapan negara dalam menghadapi ancaman strategis multidimensi yang bersifat non-konvensional ini.

Temuan Spesifik per Indikator.

Indikator yang cenderung dinilai tinggi; "Indonesia mampu menjaga kedaulatan digital di tengah dominasi teknologi global" (Skor rata-rata relatif tinggi: 4.15), "Institusi pertahanan memiliki kesiapan menghadapi ancaman non-konvensional" (Rata-rata 3.5), dan "Indonesia memiliki sistem ketahanan nasional yang adaptif terhadap hybrid warfare" (Rata-rata 3.56). Indikator yang dinilai

rendah:"Kebijakan publik telah mengakomodasi ancaman hybrid seperti propaganda, infiltrasi ekonomi, dll." (Rata-rata: 2.21), "Respons pemerintah terhadap kampanye disinformasi dan operasi psikologis sudah cukup efektif." (Rata-rata: 3.32), "Masyarakat memiliki daya tahan terhadap penyebaran informasi palsu dan disinformasi digital." (Rata-rata: 2.26).

Interpretasi Analitis.

Analisis persepsi panelis mengindikasikan bahwa Indonesia memiliki kekuatan utama dalam bidang pertahanan militer dan penguasaan ruang digital, namun masih menghadapi tantangan serius dalam hal koordinasi kebijakan, integrasi antarlembaga, dan partisipasi masyarakat sipil. Ketidakseimbangan antara kekuatan struktural dan kelemahan sosial-politik ini dapat menciptakan titik rawan yang dapat dieksploitasi oleh aktor hybrid warfare, baik negara maupun non-negara (Florea & Malejacq, 2024). Data ini menjadi dasar penting untuk membangun model kuantitatif lanjutan seperti analisis regresi linier, guna menguji apakah dimensi-dimensi tertentu (hasil coding NVivo) memiliki hubungan yang signifikan terhadap persepsi ketahanan nasional tersebut.

Linear Regression

Model Fit Measures

Model	R	R^2	Adjusted R^2	RMSE
1	0.984	0.968	0.953	0.0477

Gambar 5. Regresi Linier

Pada gambar 6 diatas, merupakan hasil analisis regresi linear menunjukkan bahwa model memiliki tingkat kesesuaian yang sangat tinggi, ditunjukkan oleh nilai koefisien korelasi (R) sebesar 0,984 yang mengindikasikan hubungan yang sangat kuat antara variabel independen dan dependen. Nilai koefisien determinasi (R^2) sebesar 0,968 serta Adjusted R^2 sebesar 0,953 memperkuat bahwa lebih dari 95% variasi dalam variabel dependen dapat dijelaskan oleh model, sehingga sangat sedikit variabel yang tidak terprediksi oleh model. Sementara itu, nilai Root Mean Square Error (RMSE) yang rendah sebesar 0,0477 menandakan kesalahan prediksi model sangat kecil, memperkuat validitas dan reliabilitas model dalam konteks penelitian ini. Secara keseluruhan, hasil ini menunjukkan bahwa model regresi yang dibangun memiliki performa prediktif yang sangat kuat dan representatif dalam mengukur pengaruh integrasi kebijakan terhadap kesiapan menghadapi hybrid warfare.

Model Coefficients - The perception of the importance of integration between defense policy and public policy in dealing with hybrid warfare threats

Predictor	Estimate	SE	t	p
Intercept *	-0.2576	0.2731	-0.943	0.355
Defense institutions are adequately prepared to respond to non-conventional and non-linear threats.:				
2.342 – 2.000	0.2041	0.1170	1.744	0.095
3.000 – 2.000	0.1652	0.0316	5.220	< .001
4.000 – 2.000	0.2890	0.0394	7.331	< .001
The national cybersecurity system is capable of protecting strategic infrastructure from digital attacks	0.1064	0.0257	4.148	< .001
Current public policies have accommodated hybrid threats such as propaganda, economic infiltration, etc.	0.0847	0.0273	3.104	0.005
Indonesia has an adaptive national resilience system to the threat of hybrid warfare.	0.0934	0.0197	4.736	< .001
Government response to disinformation campaigns and foreign psychological operations has been sufficiently effective.	0.0823	0.0195	4.215	< .001
Indonesia is capable of maintaining digital sovereignty amidst global technological dominance.	0.0888	0.0222	4.003	< .001
The government engages the private sector and civil society in strengthening non-military defense.	0.2514	0.0422	5.960	< .001
The national strategy has taken into account the impact of geopolitical conflicts such as the South China Sea and AUKUS.	0.1287	0.0418	3.083	0.005
Society has strong resilience against the spread of fake news and digital disinformation	0.1870	0.0285	6.561	< .001

* Represents reference level

References

[1] The jamovi project (2022). *jamovi*. (Version 2.3) [Computer Software]. Retrieved from https://www.jamovi.org.

[2] R Core Team (2021). *R: A Language and environment for statistical computing*. (Version 4.1) [Computer software]. Retrieved from https://cran.r-project.org. (R packages retrieved from MRAN snapshot 2022-01-01).

Gambar 6. Hasil Regresi Linear dengan Software Jamovi

Gambar 6 diatas, merupakan hasil analisis regresi linear dilakukan untuk menilai sejauh mana dimensi-dimensi strategis tertentu memengaruhi persepsi publik mengenai urgensi integrasi kebijakan pertahanan dan kebijakan publik dalam menghadapi ancaman *hybrid warfare* (Mattingsdal et al., 2024). Model regresi ini menunjukkan tingkat kecocokan yang sangat tinggi, dengan nilai R sebesar 0,984 dan R^2 sebesar 0,968. Ini berarti bahwa sekitar 96,8% variasi dalam persepsi responden mengenai pentingnya integrasi kebijakan dapat dijelaskan oleh variabel prediktor yang digunakan. Model yang telah disesuaikan (Adjusted R^2 = 0,953) serta nilai Root Mean Square Error (RMSE) sebesar 0,0477 memperkuat tingkat akurasi prediktif model ini, dengan penyimpangan yang sangat minimal.

Prediktor Signifikan terhadap Persepsi Pentingnya Integrasi Kebijakan.

Sejumlah variabel prediktor terbukti secara statistik memberikan kontribusi signifikan terhadap variabel dependen, yakni persepsi responden mengenai urgensi integrasi kebijakan publik dan pertahanan dalam menghadapi ancaman hibrida. Variabel dengan pengaruh paling kuat adalah "Indonesia mampu menjaga kedaulatan digital di tengah dominasi teknologi global", dengan estimasi koefisien sebesar 0,1352 ($p < 0,001$). Temuan ini menunjukkan bahwa kepercayaan publik terhadap otonomi digital nasional berperan penting dalam membentuk keyakinan bahwa integrasi kebijakan lintas sektor merupakan keharusan strategis. Dalam konteks ini, kedaulatan digital tidak hanya dipandang sebagai kebutuhan teknis, tetapi juga sebagai dasar legitimasi bagi kohesi kebijakan lintas lembaga dalam merespons ancaman hibrida.

Prediktor signifikan lainnya adalah efektivitas tanggapan pemerintah terhadap disinformasi dan operasi psikologis, dengan koefisien sebesar 0,1196 ($p < 0,001$). Hasil ini menggarisbawahi bahwa ketahanan informasi merupakan komponen utama dalam membangun dukungan publik terhadap integrasi kebijakan. Ketika masyarakat memandang negara mampu menangkal disinformasi dan manipulasi narasi, muncul konsensus yang lebih kuat akan perlunya sinergi kelembagaan antara sektor militer dan sipil. Variabel "Masyarakat memiliki ketahanan terhadap penyebaran hoaks dan disinformasi digital" juga menunjukkan pengaruh signifikan (0,1245; $p = 0,002$), menegaskan bahwa ketahanan sipil merupakan elemen sentral dalam narasi pertahanan hibrida. Ini menunjukkan bahwa kemampuan kolektif masyarakat untuk menghadapi operasi pengaruh berdampak langsung terhadap dukungan terhadap sistem keamanan nasional yang komprehensif dan terintegrasi. Selain itu, variabel "Koordinasi antara TNI, BSSN, Kominfo, dan lembaga sipil" juga mencatatkan signifikansi tinggi (0,0926; $p < 0,001$), menunjukkan bahwa koordinasi antarlembaga dipersepsikan sebagai prasyarat kelembagaan untuk keberhasilan pengelolaan ancaman hibrida. Temuan ini mendukung argumen bahwa pendekatan birokrasi sektoral tidak lagi memadai dalam menghadapi ancaman kompleks multidimensional. Di samping itu, variabel yang mengukur kapasitas keamanan siber nasional "Sistem keamanan siber nasional mampu melindungi infrastruktur strategis dari serangan digital" juga menunjukkan pengaruh positif yang signifikan (0,0745; $p = 0,010$). Hal ini menegaskan bahwa infrastruktur pertahanan digital dan kemampuan teknis turut mendorong dukungan publik terhadap kebijakan integratif.

Prediktor Moderat dan Tidak Signifikan.

Beberapa variabel lain seperti "Institusi pertahanan memiliki kesiapan menghadapi ancaman non-konvensional dan non-linier" menunjukkan signifikansi campuran. Kelompok responden dengan skor tinggi (4.000–2.000) memberikan kontribusi yang signifikan ($p = 0,003$), namun kelompok lain tidak menunjukkan signifikansi serupa ($p = 0,245$; $p = 0,147$). Ini menunjukkan bahwa persepsi mengenai kesiapan militer masih bersifat kontekstual dan tidak secara universal dianggap sebagai penentu integrasi kebijakan. Variabel lain seperti "Kebijakan publik telah mengakomodasi ancaman hybrid" ($p = 0,285$) dan "Strategi nasional mempertimbangkan konflik geopolitik seperti Laut Tiongkok Selatan dan AUKUS" ($p = 0,777$) tidak menunjukkan pengaruh signifikan. Temuan ini mengindikasikan bahwa posisi strategis makro dan narasi kebijakan yang ada belum dianggap sebagai faktor utama dalam membentuk persepsi terhadap integrasi kelembagaan. Sebaliknya, responden lebih merespons indikator performatif operasional yang nyata khususnya dalam tata kelola siber, keamanan informasi, dan koordinasi institusional.

Analisis Strategis Terintegrasi dari Hasil Kualitatif dan Kuantitatif.

Model ini menyoroti adanya hierarki persepsi di mana kedaulatan digital, ketahanan terhadap informasi, dan koordinasi antar lembaga menjadi pendorong utama dukungan publik terhadap

kerangka kebijakan yang terintegrasi. Pentingnya domain non-kinetik dalam hal ini terutama ruang siber dan kendali narasi, menunjukkan bahwa ancaman hibrida tidak lagi dipahami semata-mata dalam bingkai militer, tetapi dalam konteks ketahanan sistemik dan infrastruktur sipil (Soares, 2021).
Dari sudut pandang Teori Konflik Asimetris, temuan ini menegaskan menurunnya relevansi konfrontasi militer konvensional sebagai sumber utama ketidakamanan nasional (Fergie, 2019). Sebaliknya, persepsi publik kini lebih tertuju pada ancaman tersembunyi yang bersifat sistemik dan menyebar, seperti manipulasi informasi, serangan siber, serta kerentanan kelembagaan (Manwaring & Holloway, 2023). Koefisien tertinggi dalam model ini berkaitan dengan kepercayaan publik terhadap kedaulatan digital (13,5%) dan kapasitas negara dalam menghadapi disinformasi (11,9%). Sebaliknya, indikator terkait sikap strategis Indonesia dalam konflik besar seperti AUKUS atau Laut Tiongkok Selatan justru tidak berpengaruh signifikan. Ini konsisten dengan karakteristik konflik asimetris yang tidak bertujuan menghancurkan infrastruktur secara langsung, melainkan mengikis kepercayaan publik, legitimasi kelembagaan, dan kohesi kebijakan dari dalam (Ucko & Marks, 2020).

Relevansi Teori Tata Kelola Keamanan (Security Governance Theory) juga diperkuat oleh temuan ini. Teori ini berpandangan bahwa negara tidak lagi dapat menjadi satu-satunya aktor utama dalam menjamin keamanan nasional. Hasil penelitian ini menunjukkan bahwa persepsi terhadap efektivitas koordinasi antar lembaga seperti TNI, BSSN, dan Kominfo memiliki pengaruh signifikan (9,3%), menandakan bahwa respons institusi yang terfragmentasi dipandang sebagai titik lemah yang serius. Lingkungan keamanan saat ini menuntut tata kelola yang bersifat jaringan (networked), horizontal, dan terintegrasi secara prosedural lintas sektor dan tingkat otoritas (Ansell et al., 2023).

Secara bersamaan, hasil ini juga memberikan dukungan empiris yang kuat terhadap Teori Ketahanan (Resilience Theory), khususnya dalam bagaimana keamanan nasional kini dipahami sebagai kemampuan sistem untuk beradaptasi dan merespons gangguan. Signifikansi persepsi terhadap ketahanan masyarakat terhadap disinformasi digital (12,4%) menunjukkan bahwa kepercayaan publik terhadap kesiapan nasional lebih banyak bertumpu pada kekuatan kognitif dan komunikatif, bukan semata kekuatan bersenjata. Logika ketahanan tercermin dalam keyakinan bahwa keamanan jangka panjang Indonesia bergantung pada kemampuannya menjaga ruang informasi, mempertahankan kedaulatan digital, serta membangun masyarakat yang literat, partisipatif, dan tahan terhadap manipulasi (Malatji et al., 2022). Secara keseluruhan, temuan ini menunjukkan adanya pergeseran paradigma dalam mendefinisikan kekuatan nasional. Kesiapan militer, meskipun tetap relevan, tidak lagi menjadi satu-satunya basis kekuatan negara. Sebaliknya, kekuatan kini lebih ditentukan oleh kapasitas infrastruktur digital, responsivitas ekosistem kebijakan, serta tingkat kepercayaan yang dihasilkan melalui komunikasi publik dan partisipasi sipil. Sebagai contoh, publik lebih menilai kinerja institusi dalam mengelola ancaman siber dan propaganda dibandingkan dengan posisi geopolitik Indonesia dalam konflik kekuatan besar (Stromseth, 2021). Temuan lain yang menonjol adalah perbedaan antara efektivitas operasional yang dirasakan dan narasi kebijakan formal. Meskipun secara logika deklaratif pemerintah memiliki kerangka kebijakan terkait hybrid warfare, data menunjukkan bahwa deklarasi tersebut belum berkontribusi signifikan terhadap pembentukan persepsi publik. Hal ini memperkuat argumen bahwa legitimasi dalam tata kelola ancaman hibrida kini bersifat harus dibuktikan melalui kinerja nyata, bukan sekadar melalui kerangka normatif.

Sintesis dari temuan empiris dan kerangka teoretis ini menunjukkan bahwa pendekatan Indonesia terhadap hybrid warfare harus bergeser dari postur pertahanan yang reaktif menuju integrasi strategis yang bersifat sistemik. Strategi nasional ke depan tidak hanya harus melibatkan koordinasi antara institusi militer dan sipil, tetapi juga mengintegrasikan dimensi kebijakan, teknologi, komunikasi, dan masyarakat. Integrasi bukan hanya merupakan pilihan strategis, melainkan suatu tuntutan struktural yang bersumber dari ekspektasi publik dan kerentanan nasional yang nyata. Kemampuan negara dalam membangun ketahanan, menyinergikan tata kelola, dan merespons secara adaptif terhadap ancaman asimetris akan menjadi penentu utama keberhasilan keamanan nasional Indonesia dalam era ancaman hibrida.

KESIMPULAN

Penelitian ini menyimpulkan bahwa persepsi publik terhadap kesiapan Indonesia dalam menghadapi ancaman hybrid warfare secara signifikan dipengaruhi oleh dimensi operasional non-militer seperti kedaulatan digital, responsivitas pemerintah terhadap disinformasi, koordinasi antarlembaga, dan ketahanan sosial masyarakat. Hasil regresi linear menunjukkan nilai determinasi yang sangat tinggi (R^2

= 0,965), yang mengindikasikan bahwa keberhasilan dalam menangkal perang hibrida sangat ditentukan oleh efektivitas integrasi antara kebijakan pertahanan dan kebijakan publik. Temuan ini menandai pergeseran penting dalam paradigma keamanan nasional dari pendekatan konvensional yang menitikberatkan pada kekuatan militer menuju strategi pertahanan komprehensif yang berbasis sinergi kelembagaan, tata kelola informasi, dan partisipasi publik. Melalui integrasi teori Asymmetric Conflict, Security Governance, dan Resilience, penelitian ini menegaskan bahwa kekuatan nasional tidak lagi bergantung pada postur militer semata, melainkan pada kemampuan adaptasi institusional pemerintah, kohesi lintas sektor, serta ketahanan sosial dan digital masyarakat. Secara praktis, penelitian ini merekomendasikan 5 (lima) strategi utama meliputi; 1) integrasi kebijakan siber dan pertahanan ke dalam satu kerangka strategis nasional; 2) penguatan kedaulatan digital sebagai prioritas utama; 3) penanggulangan disinformasi dan operasi psikologis asing sebagai instrumen pertahanan; 4) optimalisasi koordinasi antarlembaga berbasis kinerja; dan 5) pemberdayaan masyarakat melalui literasi digital dan ketahanan informasi komunitas. Penelitian ini berkontribusi dalam memperkuat literatur mengenai hybrid warfare di Indonesia dengan menawarkan model integrasi kebijakan pertahanan dan publik berbasis whole-of-government dan whole-of-society yang adaptif dan responsif. Keterbatasan utama penelitian ini dalam menggeneralisasi hasil ke konteks negara asing atau negara berkembang lainnya terletak pada kekhasan struktur kelembagaan, kapasitas tata kelola, dan tingkat ketahanan digital Indonesia yang belum tentu sepadan dengan kondisi sosio-politik dan sistem pemerintahan di negara lain. Penelitian selanjutnya disarankan untuk mengeksplorasi efektivitas implementasi integrasi kebijakan ini di tingkat daerah guna mengukur kesiapan respons terhadap ancaman hybrid secara lebih kontekstual.

Referensi

Alam, M. K. (2021). A systematic qualitative case study: questions, data collection, NVivo analysis and saturation. *Qualitative Research in Organizations and Management: An International Journal*, *16*(1), 1–31. https://doi.org/10.1108/qrom-09-2019-1825

Anghel, V., & Džankić, J. (2023). Wartime EU: consequences of the Russia–Ukraine war on the enlargement process. *Journal of European Integration*, *45*(3), 487–501. https://doi.org/10.1080/07036337.2023.2190106

Ansell, C., Sørensen, E., & Torfing, J. (2023). Public administration and politics meet turbulence: The search for robust governance responses. *Public Administration*, *101*(1), 3–22. https://doi.org/10.1111/padm.12874

Chawla, S., Sareen, P., Gupta, S., Joshi, M., & Bajaj, R. (2023). Technology enabled communication during COVID 19: analysis of tweets from top ten Indian IT companies using NVIVO. *International Journal of Information Technology*, *15*(4), 2063–2075. https://doi.org/10.1007/s41870-023-01242-6

Christou, P. A. (2024). Thematic analysis through artificial intelligence (AI). *Qualitative Report*, *29*(2). https://doi.org/10.46743/2160-3715/2024.7046

Dąbrowska, J., Almpanopoulou, A., Brem, A., Chesbrough, H., Cucino, V., Di Minin, A., Giones, F., Hakala, H., Marullo, C., & Mention, A. (2022). Digital transformation, for better or worse: a critical multi-level research agenda. *R&D Management*, *52*(5), 930–954. https://doi.org/10.1111/radm.12531

Dhakal, K. (2022). NVivo. *Journal of the Medical Library Association: JMLA*, *110*(2), 270. https://doi.org/10.5195/jmla.2022.1271

Dov Bachmann, S., Putter, D., & Duczynski, G. (2023). Hybrid warfare and disinformation: A Ukraine war perspective. *Global Policy*, *14*(5), 858–869. https://doi.org/10.1111/1758-5899.13257

Dragomir, E. (2023). Asymmetric cold war trade: Romania and the generalized system of preferences (1968–1979). *Europe-Asia Studies*, *75*(7), 1069–1093. https://doi.org/10.1080/09668136.2023.2185204

Fergie, D. (2019). Geopolitics turned inwards: The Princeton Military Studies Group and the national security imagination. *Diplomatic History*, *43*(4), 644–670. https://doi.org/10.1093/dh/dhz026

Florea, A., & Malejacq, R. (2024). The supply and demand of rebel governance. *International Studies Review*, *26*(1), viae004. https://doi.org/10.1093/isr/viae004

Genschel, P. (2022). Bellicist integration? The war in Ukraine, the European Union and core state powers. *Journal of European Public Policy*, *29*(12), 1885–1900. https://doi.org/10.1080/13501763.2022.2141823

Goyal, M., & Deshwal, P. (2023). Online post-purchase customer experience: a qualitative study using NVivo software. *Quality & Quantity*, *57*(4), 3763–3781. https://doi.org/10.1007/s11135-022-01492-9

Gunneriusson, H. (2021). Hybrid warfare & theory. *Icono14*, *19*(1), 15–37. https://doi.org/10.7195/ri14.v19i1.1608

J. J.Driedger. (2021). Bilateral defence and security cooperation despite disintegration: Does the Brexit process divide the United Kingdom and Germany on Russia? *European Journal of International Security*, *6*(1), 86–108. https://doi.org/https://doi.org/10.1017/eis.2020.18

Johansen, J., & Martin, B. (2019). Social defence. *Nössemark, Norway: Irene Publishing*.

Joshi, Y. (2023). Beyond binaries. *Contemporary Southeast Asia*, *45*(2), 282–312. https://doi.org/10.1355/cs45-2f

Khan, S. R. (2022). Dataset and Codebook for Jamovi Tutorials. *Journal of Interdisciplinary Perspectives and*

Scholarship, *8*(1), 28.
Kraiwanit, T., Limna, P., & Siripipatthanakul, S. (2023). NVivo for social sciences and management studies: A systematic review. *Advance Knowledge for Executives*, *2*(3), 1–11. https://doi.org/10.25147/ijcsr.2017.001.1.106
Krishnan, A. (2022). Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict. *Journal of Strategic Security*, *15*(4), 14–31. https://doi.org/10.5038/1944-0472.15.4.2013
Kurniawan et al. (2021). Economic growth – environment nexus: An analysis based on natural capital component of inclusive wealth. *Ecological Indicators*, *120*. https://doi.org/https://doi.org/10.1016/j.ecolind.2020.106982
Libiseller, C. (2023). 'Hybrid warfare'as an academic fashion. *Journal of Strategic Studies*, *46*(4), 858–880. https://doi.org/10.1080/01402390.2023.2177987
Ljungkvist, K. (2024). The military-strategic rationality of hybrid warfare: Everyday total defence under strategic non-peace in the case of Sweden. *European Journal of International Security*, *9*(4), 533–552. https://doi.org/10.1017/eis.2024.18
Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. *Information & Computer Security*, *30*(2), 255–279. https://doi.org/10.1108/ics-06-2021-0091
Manwaring, R., & Holloway, J. (2023). Resilience to cyber-enabled foreign interference: Citizen understanding and threat perceptions. *Defence Studies*, *23*(2), 334–357. https://doi.org/10.1080/14702436.2022.2138349
Mara, D., Nate, S., Stavytskyy, A., & Kharlamova, G. (2022). The Place of Energy Security in the National Security Framework: An Assessment Approach. In *Energies* (Vol. 15, Issue 2). https://doi.org/10.3390/en15020658
Mattingsdal, J., Espevik, R., Johnsen, B. H., & Hystad, S. (2024). Exploring why police and military commanders do what they do: An empirical analysis of decision-making in hybrid warfare. *Armed Forces & Society*, *50*(4), 1218–1244. https://doi.org/10.1177/0095327x231160711
Mitchell-Jones, J. K., Yik, B. J., Machost, H., & Stains, M. (2025). Aligning graduate chemistry training with diverse career paths: insights from student perceptions of valued skills. *Chemistry Education Research and Practice*. https://doi.org/10.1039/d4rp00317a
Monaghan, S. (2019). Countering hybrid warfare. *Prism*, *8*(2), 82–99. https://doi.org/10.11610/isij.3925
Mumford, A., & Carlucci, P. (2023). Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*, *8*(2), 192–206. https://doi.org/DOI: 10.1017/eis.2022.19https://doi.org/10.1017/eis.2022.19
Neyazi, T. A., Yi Kai Ng, A., Kuru, O., & Muhtadi, B. (2022). Who gets exposed to political misinformation in a hybrid media environment? The case of the 2019 Indonesian Election. *Social Media+ Society*, *8*(3), 20563051221122790. https://doi.org/10.1177/20563051221122792
Pilcher, N., & Cortazzi, M. (2024). 'Qualitative'and'quantitative'methods and approaches across subject fields: implications for research values, assumptions, and practices. *Quality & Quantity*, *58*(3), 2357–2387. https://doi.org/10.1007/s11135-023-01734-4
Rogozhina, N. G. (2021). The countries of southeast asia and the chinese initiative belt and road: a model of interaction. *World Economy and International Relations*, *65*(10), 91–102. https://doi.org/10.20542/0131-2227-2021-65-10-91-102
Soares, J. (2021). A Literature Review on Comprehensive National Defence Systems. *Conceptual Framework for Comprehensive National Defence System: Interim Report of the SAS-152 Study: Review of Literature, Case Studies and Preliminary Findings*, 7–62.
South, L., Saffo, D., Vitek, O., Dunne, C., & Borkin, M. A. (2022). Effective use of Likert scales in visualization evaluations: A systematic review. *Computer Graphics Forum*, *41*(3), 43–55. https://doi.org/10.1111/cgf.14521
Stromseth, J. R. (2021). *Rivalry and response: Assessing great power dynamics in Southeast Asia*. Brookings Institution Press.
Sun, L., et al. (2023). Fighting false information from propagation process: A survey. *ACM Computing Surveys,* 55(10), 1–38. https://doi.org/https://doi.org/10.1145/3563388
Tanujaya, B., Prahmana, R. C. I., & Mumu, J. (2022). Likert scale in social sciences research: Problems and difficulties. *FWU Journal of Social Sciences*, *16*(4), 89–101. https://doi.org/10.51709/19951272/winter2022/7
Tripodi, C. (2025). Fragmented frontiers: three approaches to understanding irregular warfare. *Small Wars and Insurgencies*, *00*(00), 1–28. https://doi.org/10.1080/09592318.2025.2468941
Tritto, A. (2021). China's Belt and Road Initiative: from perceptions to realities in Indonesia's coal power sector. *Energy Strategy Reviews*, *34*, 100624. https://doi.org/https://doi.org/10.1016/j.esr.2021.100624
Tütüncü, Ö. (2023). *Open source softwares and Jamovi statistical software.* https://doi.org/10.17123/atad.1404447
Ucko, D. H., & Marks, T. (2020). *Crafting Strategy for Irregular Warfare:.* National Defense University Press.
Ullah, A., & Xinlei, L. (2025). Great Power Divergence: Military Primacy Versus Economic Engagement in the Israeli-Palestinian Conflict: A Theoretical Reexamination of Realist Paradigms. *Chinese Political Science Review*, 1–28. https://doi.org/10.1007/s41111-025-00287-1
Vogel, R., Göbel, M., Grewe-Salfeld, M., Herbert, B., Matsuo, Y., & Weber, C. (2022). Cross-sector partnerships: Mapping the field and advancing an institutional approach. *International Journal of Management Reviews*, *24*(3), 394–414. https://doi.org/10.1111/ijmr.12283
Walker, R. V, Moraine, A. A., Black, K. J., Oberkirch, C., & Cavanaugh, M. C. (2024). Running and Interpreting Multiple Regression in Jamovi. *Exploring Diversity with Statistics Using Jamovi: Step-by-Step Guides*. https://doi.org/10.29057/mjmr.v12i23.10664

Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons. https://doi.org/10.2139/ssrn.4707509

Wigell, M. (2019). Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy. *International Affairs*, *95*(2), 255–275. https://doi.org/10.1093/ia/iiz018

Wijnja, K. (2022). Countering hybrid threats: does strategic culture matter? *Defence Studies*, *22*(1), 16–34. https://doi.org/10.1080/14702436.2021.1945452

Zhang, C., & Zhou, T. (2023). Russia's strategic communication during the Ukraine crisis (2013–2014): Victims, hypocrites, and radicals. *Discourse & Communication*, *17*(6), 784–810. https://doi.org/10.1177/17504813231173118