LEBAH
ISSN 1412-8128 (Print), 2964-9056 (Online) | Volume 18, No. 3 May (2025)
Diterbitkan oleh: Institut Hukum Sumberdaya Alam (IHSA Institute)

Model integrasi kebijakan pertahanan dan kebijakan publik mengatasi ancaman perang hibrida guna meningkatkan pertahanan negara

Trias Wijanarko[1], Asep Adang Supriyadi[2], Guntur Eko Saputro[3], Faonaso Harefa[4], Yuli Kartiningsih[5], Adam Mardamsyah[6]
[1),2),3),4),5),6)]Universitas Pertahanan, Matraman, Jakarta Timur, Jakarta, Indonesia

Article Info

Article history

Received : May 12, 2025
Revised : May 27,2025
Accepted : May 31, 2025

Abstrak

Dalam era globalisasi yang kompleks, ancaman terhadap keamanan nasional tidak lagi bersifat konvensional, melainkan cenderung mengarah pada bentuk hybrid warfare *yang menggabungkan aspek militer, siber, ekonomi, sosial, dan politik. Penelitian ini menyoroti pentingnya integrasi antara kebijakan pertahanan dan kebijakan publik sebagai respons strategis terhadap dinamika ancaman tersebut. Globalisasi telah menciptakan jaringan ketergantungan antarnegara, sehingga kebijakan pertahanan tidak dapat lagi berdiri sendiri, melainkan harus bersinergi dengan kebijakan publik yang mampu menjawab akar masalah seperti ketimpangan sosial dan ketidakpuasan politik. Selain itu, kemajuan teknologi seperti kecerdasan buatan, sistem drone, dan serangan siber turut membentuk ulang strategi pertahanan, sehingga menuntut adanya kebijakan yang adaptif, etis, dan terintegrasi. Kerja sama internasional dan keterlibatan masyarakat sipil menjadi komponen penting dalam menyusun kebijakan yang legitimatif dan berkelanjutan. Penelitian ini menggunakan pendekatan kualitatif deskriptif melalui kegiatan brainstorming dalam pengabdian kepada masyarakat oleh mahasiswa doktoral Universitas Pertahanan, untuk menggali pandangan para pemangku kepentingan terkait integrasi kebijakan. Temuan ini merekomendasikan strategi kolaboratif, partisipatif, dan berbasis inovasi untuk membangun sistem keamanan nasional yang tangguh dalam menghadapi ancaman* hybrid warfare *yang terus berkembang.*

Kata Kunci:

Globalisasi;
Hybrid Warfare;
Integrasi Kebijakan;
Teknologi Pertahanan.

Abstract

In a complex era of globalization, threats to national security are no longer conventional, but they tend to lead to hybrid warfare forms that combine military, cyber, economic, social, and political aspects. This study highlights the importance of integration between defense policies and public policies as a strategic response to the dynamics of the threat. Globalization has created a network of dependence between countries so that defense policies can no longer stand alone but must synergize with public policies that are able to answer the root of problems such as social inequality and political dissatisfaction. In addition, technological advances such as artificial intelligence, drone systems, and cyber attacks helped reform defense strategies, thus demanding adaptive, ethical, and integrated policies. International cooperation and civil society involvement are important components in developing legitimate and sustainable policies. This study uses a descriptive qualitative

approach through brainstorming activities in community service by doctoral students of Defense University to explore the views of stakeholders related to policy integration. These findings recommend collaborative, participatory, and innovative strategies to build a strong national security system in dealing with the growing threat of hybrid warfare.

Corresponding Author:

Faoanso Harefa,
Managemen Pertahanan
Universitas Pertahanan
Jl. Salemba Raya Nomor 14, Kenari Kec. Senen Jakarta Pusat 10440, Jakarta Pusat, Indonesia
Faonaso.harefa@doktoral.idu.ac.id

PENDAHULUAN

Dalam beberapa dekade terakhir, keamanan nasional mengalami transformasi yang signifikan seiring dengan berkembangnya ancaman *hybrid warfare*. Perubahan ini dipicu oleh kemajuan teknologi, globalisasi, serta perubahan dinamika politik dan ekonomi global. *Hybrid warfare* merupakan bentuk ancaman yang kompleks dan tidak lagi mengandalkan konfrontasi militer secara langsung. Sebaliknya, ancaman ini melibatkan berbagai aspek non-konvensional seperti serangan siber, propaganda digital, disinformasi, manipulasi ekonomi, dan infiltrasi politik. Bentuk-bentuk baru *hybrid warfare* atau operasi siber berkembang secara dinamis, dimana serangan siber menimbulkan tantangan unik, karena sulit untuk mengaitkan dan membuktikannya dibandingkan dengan tindakan perang tradisional (Cremer et al., 2024). Berbeda dengan perang konvensional yang memiliki garis pertempuran yang jelas, hybrid warfare bersifat asimetris dan tersembunyi. Serangan dapat dilakukan oleh aktor negara maupun non-negara dengan tujuan untuk melemahkan stabilitas internal suatu negara tanpa perlu melibatkan konflik fisik secara terbuka. Hal Ini menunjukkan perlunya kesinambungan antara Doktrin Keamanan Nasional masa lalu dan wacana militer saat ini dan ideologi keamanan nasional dan tatanan sosial (Achugar & Fried Amilivia, 2024). Sementara berbagai definisi hybrid warfare telah muncul, biasanya dilihat sebagai kombinasi dari perang konvensional, perang tidak teratur, terorisme, dan berbagai jenis kriminalitas yang mengancam negara (Tin et al., 2023). Dinamika keamanan nasional beberapa waktu terakhir menunjukkan bahwa hybrid warfare terus berkembang sejalan dengan perkembangan ilmu pengetahuan dan teknologi dan menjadi tantangan bagi semua negara untuk mengantisipasi dan menghadapinya. Indonesia, sebagai negara kepulauan yang kaya akan keberagaman etnis, agama, dan budaya, memiliki posisi strategis yang menjadikannya target potensial dalam konteks hybrid warfare. Dengan lebih dari 270 juta penduduk yang tersebar di lebih dari 17.000 pulau, Indonesia tidak hanya menghadapi tantangan dalam menjaga keutuhan wilayah, tetapi juga dalam mempertahankan stabilitas sosial dan politik(Abd Al Ghaffar, 2024).

Berkembangnya *hybrid warfare*, konsep pertahanan harus mengalami perubahan mendasar. Proses pembuatan kebijakan luar negeri dan pertahanan sangat dilembagakan dan konsensual namun tetap adaptif (Amorim Neto & Anselmo, 2023). Ketahanan nasional tidak lagi hanya bergantung pada kekuatan militer, tetapi juga pada ketahanan informasi, teknologi, dan ekonomi. Salah satu tantangan terbesar dalam kebijakan pertahanan terhadap *hybrid warfare* adalah sulitnya mengidentifikasi sumber ancaman. Dalam perang konvensional, musuh dapat dengan mudah dikenali melalui penggunaan kekuatan bersenjata. Sebaliknya, dalam *hybrid warfare*, musuh sering kali beroperasi melalui aktor-aktor bayangan, serangan siber tanpa tanda tangan yang jelas, serta propaganda yang menyebar secara luas melalui media sosial. Pembuat kebijakan pertahanan menjadi semakin khawatir tentang konflik di "zona abu-abu" antara perdamaian dan perang (Gannon et al., 2024).

Indonesia perlu membangun strategi pertahanan yang adaptif dan fleksibel dalam menghadapi *hybrid warfare*. Ini mencakup penguatan sistem pertahanan siber, peningkatan kapasitas intelijen dalam mendeteksi dan menangkal serangan non-konvensional, serta penguatan kapasitas diplomasi pertahanan untuk membangun kerja sama dengan negara-negara lain dalam menghadapi ancaman

bersama. Beberapa deklarasi bilateral, bagaimanapun, juga berisi tujuan di luar kebijakan luar negeri, keamanan dan pertahanan (Meislová & Glencross, 2023).

Kebijakan pertahanan, kebijakan publik juga berperan penting dalam menangkal *hybrid warfare*. Kebijakan publik berperan sangat penting dalam penegakan hukum dan sektor sosial (Filatova et al., 2023).. Ketika sistem perbankan diserang, bukan hanya transaksi keuangan yang terhambat, tetapi juga kepercayaan masyarakat terhadap stabilitas ekonomi dapat terguncang. Hal ini dapat menyebabkan dampak jangka panjang yang merugikan bagi perekonomian nasional. Kebijakan publik juga harus mencakup regulasi terhadap penggunaan teknologi dan media sosial untuk mencegah penyalahgunaan yang dapat digunakan sebagai alat *hybrid warfare*. Pemerintah perlu bekerja sama dengan sektor swasta dan penyedia layanan internet untuk meningkatkan keamanan siber serta mengembangkan mekanisme yang efektif dalam mendeteksi dan mengatasi ancaman non-konvensional yang menyasar masyarakat. Fokus yang lebih besar pada persimpangan kebijakan yang digunakan untuk mengatasi masalah kebijakan tertentu atau mencapai tujuan kebijakan dengan demikian diperlukan jika studi kebijakan publik regional dalam sistem tata kelola (Kleider & Toubeau, 2022).

Penggunaan teknologi kecerdasan buatan dan *big data analytics* dapat membantu dalam memprediksi serangan siber, mengidentifikasi kampanye disinformasi, serta mengantisipasi tekanan ekonomi yang dapat berdampak pada stabilitas nasional. Pemerintah pusat memperketat regulasi dan pengawasan untuk mengurangi ketidakpatuhan terhadap inisiatif energinya dan untuk menjaga keamanan nasional dan stabilitas sosial (Zhang, 2024).

METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif untuk mengkaji secara mendalam proses integrasi antara kebijakan pertahanan dan kebijakan publik dalam menghadapi ancaman *hybrid warfare* melalui perspektif analisis keamanan nasional. Pendekatan ini dipilih karena memungkinkan peneliti untuk memahami fenomena yang kompleks dan multidimensional secara kontekstual, terutama dalam konteks dinamika kebijakan dan respons lintas sektor terhadap ancaman yang bersifat non-linier dan tidak konvensional. Teknik pengumpulan data dilakukan melalui hasil brainstorming dalam kegiatan Pengabdian kepada Masyarakat (PKM) yang diselenggarakan oleh mahasiswa Pascasarjana Program Doktor Universitas Pertahanan (Unhan), di mana para peserta berdiskusi langsung dengan praktisi, akademisi, dan pemangku kepentingan dari berbagai instansi terkait. Interaksi ini menghasilkan data kualitatif yang kaya dan relevan, mencerminkan persepsi, pengalaman, serta tantangan integrasi kebijakan dari sudut pandang multidisiplin. Hasil brainstorming ini menjadi dasar dalam menganalisis sejauh mana kebijakan pertahanan telah diintegrasikan dengan kebijakan publik, serta mengidentifikasi faktor pendukung dan penghambat dalam membangun ketahanan nasional terhadap ancaman *hybrid warfare* yang semakin nyata di era kontestasi geopolitik dan teknologi informasi.

HASIL DAN PEMBAHASAN

Gambar 1. *Dokumentasi Penyampaian Materi Pengabdian Kepada Masyarakat (PKM)*

Hybrid Warfare dalam Perspektif Keamanan Nasional

Hybrid warfare merupakan ancaman multidimensional yang mengaburkan batas antara perang dan damai. Ada banyak definisi dan konsep yang berbeda-beda untuk memahami *hybrid warfare* (Janičatová & Mlejnková, 2021). *Hybrid warfare* dengan berbagai bentuk dapat dimanfaatkan untuk merusak tatanan demokrasi (Yanchenko et al., 2024). Keamanan nasional merupakan faktor penting bagi fungsi dan perkembangan individu, masyarakat, dan negara (Shkuta et al., 2024). Namun, seringkali lembaga keamanan nasional bertindak sangat represif atas nama keamanan negara untuk mengatasi berbagai ancaman (Kwak, 2024). Tidak jarang norma-norma demokrasi terganggu oleh alasan keamanan nasional pada berbagai kebijakan negara (Green & Denney, 2024). Pemerintah bagaimanapun harus memperkuat pendidikan keamanan nasional, meningkatkan kesadaran kepatuhan hukum dan keamanan nasional masyarakat, khususnya kaum muda (Peck et al., 2024). Masyarakat yang memiliki literasi digital yang tinggi akan lebih tahan terhadap propaganda dan disinformasi, sehingga lebih sulit bagi aktor hibrida untuk mengeksploitasi perpecahan sosial. Keterampilan, pengetahuan, dan kemampuan seseorang atau kelompok sosial yang digunakan saat berinteraksi dengan teknologi digital digambarkan sebagai literasi digital (Cetindamar Kozanoglu & Abedin, 2021). Tema-tema yang terkait dengan literasi digital, pertimbangan etika dan sosial, serta pentingnya fitur spesifik manusia juga terbukti dan sangat ditekankan dalam literatur terkait (Firat, 2023). Intelijen yang kuat sangat diperlukan untuk mendeteksi dini ancaman hibrida yang sering kali tersembunyi di balik operasi informasi dan serangan siber. Kontra-intelijen juga harus ditingkatkan untuk mencegah infiltrasi oleh aktor asing yang dapat memanfaatkan celah dalam sistem keamanan nasional. Kegiatan kontra-intelijen bersifat strategis dan mencakup wilayah geopolitik yang luas (Tyulenev, 2021). Peningkatan kapasitas sumber daya manusia dalam bidang intelijen menjadi prioritas utama agar Indonesia mampu mengantisipasi ancaman yang bersifat dinamis. Teknologi intelijen berbasis kecerdasan buatan (*artificial intelligence*) dan analitik data perlu dikembangkan untuk meningkatkan akurasi deteksi dini ancaman. Perluasan kecerdasan buatan (AI) di berbagai sektor di seluruh dunia menuntut pemahaman tentang dampaknya terhadap generasi mendatang (Kharroubi et al., 2024).

Dengan semakin meningkatnya serangan siber terhadap infrastruktur nasional, pertahanan siber menjadi prioritas utama dalam kebijakan pertahanan modern. Peningkatan keamanan sistem digital, kerja sama dengan sektor swasta dalam perlindungan data, dan pelatihan bagi tenaga ahli siber menjadi langkah penting dalam menghadapi ancaman ini. Pengembangan strategi deteksi dini dan respons cepat terhadap serangan siber harus dilakukan melalui kolaborasi antara lembaga pemerintah dan perusahaan teknologi. Pembangunan pusat komando siber nasional yang terintegrasi dengan instansi pertahanan dan keamanan siber menjadi kebutuhan mendesak. Teknologi berbasis kecerdasan buatan (AI) secara aktif digunakan untuk tujuan pertahanan siber (Yamin et al., 2021). Berbagai ancaman mulai dari pencurian dan serangan siber dapat mengakibatkan *blocking* dan kerusakan sistem, kegagalan berjenjang dan lain sebagainya (Sahoo et al., 2021). Pengembangan Doktrin Pertahanan Hibrida (*hybrid defence*). Doktrin pertahanan nasional harus diperbarui untuk menghadapi *hybrid warfare*, termasuk operasi non-konvensional dan peperangan informasi. Militer juga perlu mengembangkan kemampuan dalam bidang kontra-propaganda dan operasi psikologis untuk melawan perang informasi yang dilakukan oleh pihak asing. Penerapan strategi *Total Defense* atau pertahanan semesta, yang melibatkan semua elemen masyarakat dalam sistem pertahanan, dinilai sudah tepat. Konsep pertahanan total merupakan upaya bersama antara pasukan militer dan struktur pertahanan sipil dalam negara pertahanan total (Antai & Hellberg, 2024). Tidak mudah menerapkan manajemen krisis dalam imlementasi pertahanan total, karena pelibatan berbagai pihak dan penentuan prioritas (Ericson & Wester, 2022).

Modernisasi alat utama sistem persenjataan (*alutsista*) menjadi elemen penting dalam meningkatkan daya tangkal Indonesia terhadap ancaman *hybrid warfare*. Pengembangan teknologi militer berbasis kecerdasan buatan (*artificial intelligence*), sistem pertahanan udara canggih, serta peningkatan kapasitas radar dan satelit diperlukan untuk memperkuat pertahanan nasional. Kerja Sama Internasional dalam Keamanan dan Pertahanan. Kerja sama internasional, yang biasanya diatur oleh organisasi antar pemerintah dan non-pemerintah, inisiatif sektor swasta, dan oleh peneliti akademis, telah meningkatkan kesejahteraan bersama untuk menghindari hasil yang tidak diinginkan di bidang teknologi lainnya (Feijóo et al., 2020). kebijakan pemerintah yang kuat dan kerja sama internasional dinilai penting untuk mendorong transisi yang lebih cepat menuju pembangunan yang berkelanjutan di berbagai sektor (Losada-Agudelo & Souyris, 2024).

Penguatan sistem *resilience* nasional, di mana masyarakat juga dilibatkan dalam menghadapi ancaman hibrida, harus menjadi bagian dari strategi pertahanan Indonesia. Konsep ketahanan nasional adalah konsep yang luas, membahas masalah keberlanjutan dan kekuatan sosial di beberapa bidang yang beragam (Kimhi et al., 2020). Reformasi Kebijakan dan Regulasi Keamanan Nasional. Pemerintah perlu menyusun kebijakan keamanan nasional yang fleksibel dan adaptif terhadap perubahan lanskap ancaman global. Revisi terhadap regulasi terkait keamanan siber, perlindungan data, serta penegakan hukum terhadap aktor yang terlibat dalam *hybrid warfare* harus dilakukan untuk meningkatkan efektivitas respons nasional. Koordinasi antar-lembaga, termasuk Badan Siber dan Sandi Negara (BSSN), TNI, Polri, dan kementerian terkait, harus diperkuat agar kebijakan pertahanan dapat diimplementasikan secara efektif.

Peran Kebijakan Publik dalam Keamanan Nasional

Pendidikan kebangsaan dan literasi digital perlu diperkuat untuk meningkatkan daya kritis masyarakat dalam memilah informasi yang benar. Ketahanan ekonomi menjadi elemen krusial dalam menghadapi *hybrid warfare* yang sering kali menggunakan strategi pelemahan ekonomi sebagai instrumen serangan. Diversifikasi sumber daya ekonomi dan peningkatan kemandirian ekonomi nasional dapat mengurangi ketergantungan terhadap negara lain yang berpotensi menjadi ancaman. Penguatan regulasi investasi dan perdagangan penting agar tidak menjadi celah bagi aktor *hybrid warfare*. Pemerintah perlu mengembangkan kebijakan keamanan siber yang komprehensif untuk melindungi infrastruktur kritis nasional dari serangan siber. Memahami lanskap ancaman saat ini serta deteksi tepat waktu dari serangan yang akan segera terjadi adalah tujuan utama keamanan siber (Landauer et al., 2025). Keamanan siber yang kuat akan berperan sangat penting dari sebelumnya karena negara pasti akan menjadi sasaran kejahatan siber dengan tumbuhnya infrastruktur digital (Rashed et al., 2025).

Media memiliki peran strategis dalam membangun narasi nasional yang positif dan menangkal propaganda dari pihak asing. Kolaborasi antara pemerintah dan media dalam menyajikan informasi yang akurat dan kredibel kepada publik. Pengembangan teknologi berbasis kecerdasan buatan untuk mendeteksi dan menangkal konten hoaks secara otomatis. Kecerdasan buatan merupakan konsep yang telah menjadi bagian dari wacana publik selama beberapa dekade, sering digambarkan dalam film fiksi ilmiah atau perdebatan tentang bagaimana mesin cerdas akan mengambil alih dunia dalam tatanan baru (Dwivedi et al., 2021). Kebijakan Hukum dan Penegakan Keamanan Nasional. Penegakan hukum yang kuat diperlukan untuk menghadapi ancaman *hybrid warfare* yang sering kali melibatkan aktor non-negara dan metode non-konvensional. Reformasi hukum dalam menangani kasus-kasus yang berkaitan dengan keamanan siber, spionase ekonomi, serta infiltrasi politik oleh kekuatan asing. Untuk meningkatkan keadilan hukum, diperlukan perubahan pada praktik penegakan hukum, di samping reformasi hukum yang mendasar (Hulley & Young, 2024). Tantangan reformasi hukum telah menjadi tema yang konsisten dalam permasalah hukum saat ini, termasuk kontribusi dari akademisi dan pejabat yang sedang menjabat dalam organisasi hukum (Lee, 2023). Penguatan kerja sama antara lembaga hukum, kepolisian, dan intelijen dalam mendeteksi serta menangkal ancaman yang bersifat asimetris.

Ancaman *hybrid warfare* tidak hanya menjadi tanggung jawab sektor pertahanan, tetapi juga membutuhkan koordinasi yang erat antara berbagai kementerian dan lembaga. Pembentukan pusat koordinasi nasional untuk mengintegrasikan kebijakan lintas sektor dalam menangkal ancaman hibrida. Peningkatan efektivitas koordinasi antara sektor pertahanan, ekonomi, komunikasi, serta teknologi dalam menyusun kebijakan keamanan nasional. Keterlibatan Masyarakat Sipil dalam Keamanan Nasional. Partisipasi aktif masyarakat dalam kebijakan keamanan nasional menjadi faktor kunci dalam menangkal ancaman *hybrid warfare*. Dengan meningkatnya ancaman *hybrid warfare*, harus dikembangkan pengetahuan tentang kesadaran situasi dalam lingkungan kerja, di mana kesalahan manusia atau kinerja rendah dapat merugikan (Ofte & Katsikas, 2023). Diplomasi Publik sebagai Instrumen Keamanan Nasional. Pengembangan strategi komunikasi publik yang transparan untuk membangun kepercayaan masyarakat terhadap pemerintah. Dengan pendekatan yang holistik, kebijakan publik dapat menjadi komponen utama dalam membangun ketahanan nasional yang tangguh. Kami mendorong para akademisi untuk membuat asumsi mereka secara eksplisit, untuk lebih memahami potensi pemecahan masalah tata kelola swasta dan interaksinya dengan kebijakan publik (Grabs et al., 2021). Keputusan dan tindakan negara dan kebijakan publik pada konteks tertentu dapat bersifat anti-ketahanan, merusak ketahanan masyarakat dan sosial yang sudah ada dalam bentuk hubungan sosial (Haynes et al., 2024).

Hybrid warfare adalah pendekatan strategis yang komprehensif, seringkali menggabungkan aktor ancaman negara dan non-negara dalam kombinasi 'luas, kompleks, adaptif, dan seringkali sangat terintegrasi dari cara konvensional dan tidak konvensional (Dov Bachmann et al., 2023). Keamanan nasional tidak hanya bergantung pada aspek militer, tetapi juga mencakup elemen politik, ekonomi, sosial, teknologi, dan diplomasi. Oleh karena itu, sinergi antara kebijakan pertahanan dan kebijakan publik menjadi krusial dalam memperkuat ketahanan nasional. Respon terhadap COVID-19 adalah untuk mempercepat penggabungan konseptual penyakit menular yang muncul dan kesehatan masyarakat dengan biopertahanan dan biosekuriti secara eksplisit dalam konteks keamanan nasional dan militer, terutama dalam konteks program pertahanan atau militer (Kosal, 2024).

Ancaman *hybrid warfare* tidak dapat dihadapi hanya oleh satu sektor, melainkan memerlukan koordinasi lintas sektor. Konsep *hybrid warfare* berkorelasi dengan konsep perang generasi baru dalam kebijakan militer (Suchkov, 2021). Sinergi antara Sektor Militer dan Sipil dalam Keamanan Nasional. Prinsip dasar peningkatan kerja sama sipil-militer adalah menghilangkan atau meminimalkan kekurangan yang teridentifikasi dari intervensi yang telah diterapkan dalam situasi krisis, latihan, dan juga dari analisis yang dipublikasikan dari situasi krisis di dalam dan luar negeri (Tušer et al., 2021). Pengembangan model konseptual kerja sama sipil-militer di bidang ATM dan adaptasi pencapaian dari ranah sipil ke ranah militer merupakan pendekatan yang inovatif (Dymyt & Wincewicz-Bosy, 2023).

Para pemimpin populis menganggap kebijakan luar negeri sebagai kelanjutan dari politik dalam negeri, karena mereka menganggap diri mereka sebagai satu-satunya wakil rakyat yang sejati (Metawe, 2024). Diplomasi menjadi alat penting dalam mengantisipasi ancaman *hybrid warfare* yang bersumber dari aktor asing. Kebijakan Publik yang Mendukung Ketahanan Ekonomi dan Sosial. Ketahanan ekonomi menjadi faktor utama dalam menghadapi tekanan ekonomi yang merupakan bagian dari *hybrid warfare*. Pemerintah perlu memperkuat kebijakan yang mendukung stabilitas sosial dan ekonomi agar tidak mudah terpengaruh oleh strategi destabilisasi dari aktor eksternal. Penguatan sistem logistik dan ketahanan pangan nasional untuk mengurangi ketergantungan pada pihak asing. Peran Media dalam Menangkal Disinformasi dan Propaganda. Media memiliki peran krusial dalam menangkal propaganda dan menyebarkan informasi yang akurat kepada masyarakat. Pemerintah perlu bekerja sama dengan media dalam membangun narasi yang positif dan menangkal hoaks yang berpotensi melemahkan ketahanan nasional. Untuk memberikan pembangunan berkelanjutan publik, kesejahteraan bersama dan ketaatan konstitusional, banyak dokumen diadopsi untuk meningkatkan ketahanan nasional di cabang digital, keamanan, keuangan, sosial dan lainnya (Lebid et al., 2023). Keterlibatan Aktif Masyarakat dalam Sistem Keamanan Nasional. Penguatan peran organisasi masyarakat dalam menjaga stabilitas dan keamanan nasional. Perhatian khusus dalam penelitian ini diberikan pada perencanaan tata ruang dan pengembangan spasial di kota pintar ancaman utama terhadap keamanan nasional disistematiskan, terletak di bidang teknologi digital, proses sosial, dan kepentingan ekonomi yang bersinggungan erat (Sydorchuk et al., 2024). Hukum keamanan nasional modern di berbagai negara telah berkembang dalam serangkaian siklus, didorong oleh perubahan lanskap hukum dan munculnya (kembali) ancaman baru dan berbeda terhadap negara dan kepentingannya (Scott, 2024).

Reformasi di sektor pertahanan, baik dalam konteks pengurangan maupun pengeluaran sangat mempengaruhi kebijakan pertahanan (Lundberg & Rova, 2022). Meskipun integrasi kebijakan pertahanan dan kebijakan publik sangat penting dalam menghadapi ancaman *hybrid warfare*, terdapat beberapa tantangan yang harus diatasi. Karena pada dasarnya, *hybrid warfare* dapat dipahami sebagai pendekatan yang dikalibrasi menggunakan berbagai alat militer dan non-militer untuk mengacaukan, mempengaruhi, dan menumbangkan tujuan politik yang lebih luas (Davies, 2022). *Hybrid warfare* adalah konsep ambigu yang mengaburkan pemikiran strategis dan melupakan perbedaan antara perang dan perdamaian (Caliskan & Liégeois, 2021). Banyak yang berpendapat bahwa perang zona abu-abu hanyalah ekspresi tautologis dari istilah-istilah seperti *hybrid warfare*, perang generasi kelima, perang proksi, perang tidak konvensional, dan perang tidak teratur (Azad et al., 2023).

Pertama, kurangnya koordinasi antar lembaga dapat menghambat integrasi kebijakan pertahanan dan kebijakan publik (Seo et al., 2023). Keamanan siber melampaui tingkat analisis, membutuhkan pengetahuan interdisipliner yang cukup besar, dan akan dibentuk oleh ketersediaan data dan metode baru (Dunn Cavelty & Wenger, 2020). Kedua; untuk mengatasi tantangan ini, negara dapat mencari kerjasama internasional, termasuk bantuan keuangan dan teknis dari negara-negara sekutu atau organisasi internasional. Negara yang melakukan hubungan internasional telah berperan dalam membentuk alam, mengubah strata bumi dan troposfer melalui ledakan nuklir, bahkan dalam penggundulan hutan, dan polusi kimia seperti kloroflourokarbon (Crawford, 2025). Ketiga, resistensi

terhadap perubahan dapat menghambat upaya untuk mengintegrasikan kebijakan pertahanan dan kebijakan publik (Kisiliuk et al., 2024). Keempat, rendahnya standar etik dalam kebijakan publik dapat menjadi hambatan sekaligus tantangan untuk mengintegrasikan kebijakan pertahanan dan kebijakan publik.

KESIMPULAN

Dalam era globalisasi yang sarat kompleksitas, tantangan di bidang pertahanan semakin beragam dan tidak bisa hanya dihadapi dengan pendekatan militer semata. Globalisasi telah menciptakan jaringan ketergantungan antarnegara yang memperbesar dimensi internasional dari setiap isu keamanan. Oleh karena itu, kebijakan pertahanan modern perlu diintegrasikan dengan kebijakan publik secara holistik, mencakup aspek sosial, ekonomi, dan politik. Ketidakadilan sosial, kemiskinan, dan ketidakpuasan politik dapat memicu instabilitas, sehingga solusi keamanan tidak cukup hanya mengandalkan kekuatan militer, melainkan memerlukan kebijakan publik yang menyasar akar permasalahan sosial. Teknologi memainkan peran besar dalam perubahan paradigma pertahanan. Kemajuan dalam bidang siber, kecerdasan buatan, dan drone telah mengubah strategi militer global. Meskipun memberikan keuntungan strategis, teknologi juga menghadirkan tantangan baru seperti ancaman serangan siber terhadap infrastruktur kritis. Negara perlu menyusun kebijakan yang tidak hanya mendorong inovasi, tetapi juga menjamin keamanan, regulasi, dan aspek etika dalam penggunaannya. Di saat yang sama, kerja sama internasional semakin penting, terutama dalam menghadapi isu lintas batas seperti terorisme, migrasi, dan perubahan iklim. Selain negara dan teknologi, keterlibatan masyarakat sipil menjadi elemen penting dalam merancang kebijakan yang inklusif dan berkelanjutan. Partisipasi aktif dari komunitas lokal, akademisi, dan organisasi non-pemerintah memperkuat legitimasi dan efektivitas kebijakan publik. Dengan melibatkan semua pemangku kepentingan, pemerintah dapat menciptakan kepercayaan dan memperkuat stabilitas sosial.

Referensi

Abd Al Ghaffar, H. t. A. N. (2024). Government Cloud Computing and National Security. *Review of Economics and Political Science*, *9*(2), 116–133. https://doi.org/10.1108/REPS-09-2019-0125

Achugar, M., & Fried Amilivia, G. (2024). Fifty Years of Secrecy: The Politics of Oblivion and Perpetuation of the Dictatorship's Impunity in Contemporary Uruguay. *American Behavioral Scientist*. https://doi.org/10.1177/00027642241267897

Amorim Neto, O., & Anselmo, A. (2023). Presidential Activism and Success in Foreign and Defence Policy: A Study of Portugal's Premier-Presidential Regime. *Political Studies Review*. https://doi.org/10.1177/14789299231183575

Antai, I., & Hellberg, R. (2024). Identifying total defense logistics concepts: a comparative study of the Swedish pandemic response. *Journal of Humanitarian Logistics and Supply Chain Management*, *14*(2), 208–222. https://doi.org/10.1108/JHLSCM-07-2022-0084

Azad, T. M., Haider, M. W., & Sadiq, M. (2023). Understanding Gray Zone Warfare From Multiple Perspectives. *World Affairs*, *186*(1), 81–104. https://doi.org/10.1177/00438200221141101

Caliskan, M., & Liégeois, M. (2021). The concept of 'hybrid warfare' undermines NATO's strategic thinking: insights from interviews with NATO officials. *Small Wars and Insurgencies*, *32*(2), 295–319. https://doi.org/10.1080/09592318.2020.1860374

Cetindamar Kozanoglu, D., & Abedin, B. (2021). Understanding the role of employees in digital transformation: conceptualization of digital literacy of employees as a multi-dimensional organizational affordance. *Journal of Enterprise Information Management*, *34*(6), 1649–1672. https://doi.org/10.1108/JEIM-01-2020-0010

Crawford, N. C. (2025). Not redeemed from time: the deep time of world politics and the role of chronological horizons. *Australian Journal of International Affairs*, *79*(1), 10–31. https://doi.org/10.1080/10357718.2024.2424319

Cremer, F., Sheehan, B., Mullins, M., Fortmann, M., Ryan, B. J., & Materne, S. (2024). On the insurability of cyber warfare: An investigation into the German cyber insurance market. *Computers and Security*, *142*(April), 103886. https://doi.org/10.1016/j.cose.2024.103886

Davies, L. (2022). A "hybrid offensive" in the Balkans? Russia and the EU-led Kosovo-Serb negotiations. *European Security*, *31*(1), 1–20. https://doi.org/10.1080/09662839.2021.1948837

Dov Bachmann, S. D., 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

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., … Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *57*(August), 0–1. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Dymyt, M., & Wincewicz-Bosy, M. (2023). Civil-military cooperation in the field of additive manufacturing technologies in military logistics. *Systemy Logistyczne Wojsk*, *59*(2), 5–20. https://doi.org/10.37055/slw/186391

Ericson, M., & Wester, M. (2022). If I tell you I will have to kill you: secrecy in public administration in a time of securitization and militarization. *Critical Studies on Security*, *10*(1), 43–54. https://doi.org/10.1080/21624887.2022.2062926

Feijóo, C., Kwon, Y., Bauer, J. M., Bohlin, E., Howell, B., Jain, R., Potgieter, P., Vu, K., Whalley, J., & Xia, J. (2020). Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. *Telecommunications Policy*, *44*(6). https://doi.org/10.1016/j.telpol.2020.101988

Filatova, H., Tumpach, M., Reshetniak, Y., Lyeonov, S., & Vynnychenko, N. (2023). Public policy and financial regulation in preventing and combating financial fraud: a bibliometric analysis. *Public and Municipal Finance*, *12*(1), 48–61. https://doi.org/10.21511/pmf.12(1).2023.05

Firat, M. (2023). What ChatGPT means for universities: Perceptions of scholars and students. *Journal of Applied Learning and Teaching*, *6*(1), 57–63. https://doi.org/10.37074/jalt.2023.6.1.22

Gannon, J. A., Gartzke, E., Lindsay, J. R., & Schram, P. (2024). The Shadow of Deterrence: Why Capable Actors Engage in Contests Short of War. In *Journal of Conflict Resolution* (Vol. 68, Issues 2–3). https://doi.org/10.1177/00220027231166345

Grabs, J., Auld, G., & Cashore, B. (2021). *Private regulation , public policy , and the perils of adverse ontological selection*. *July 2020*, 1183–1208. https://doi.org/10.1111/rego.12354

Green, C., & Denney, S. (2024). Why do democratic societies tolerate undemocratic laws? Sorting public support for the National Security Act in South Korea. *Democratization*, *31*(1), 113–131. https://doi.org/10.1080/13510347.2023.2258082

Haynes, P., Hart, A., Eryigit-Madzwamuse, S., Wood, M., Maitland, J., & Cameron, J. (2024). The contribution of a complex systems-based approach to progressive social resilience. *Health (United Kingdom)*, *28*(5), 754–774. https://doi.org/10.1177/13634593231195784

Hulley, S., & Young, T. (2024). Joint enterprise in England and Wales: why problems persist despite legal change. *Current Issues in Criminal Justice*, 134–153. https://doi.org/10.1080/10345329.2024.2331730

Janičatová, S., & Mlejnková, P. (2021). The ambiguity of hybrid warfare: A qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities. *Contemporary Security Policy*, *42*(3), 312–344. https://doi.org/10.1080/13523260.2021.1885921

Kharroubi, S. A., Tannir, I., Abu El Hassan, R., & Ballout, R. (2024). Knowledge, Attitude, and Practices toward Artificial Intelligence among University Students in Lebanon. *Education Sciences*, *14*(8). https://doi.org/10.3390/educsci14080863

Kimhi, S., Marciano, H., Eshel, Y., & Adini, B. (2020). Community and national resilience and their predictors in face of terror. *International Journal of Disaster Risk Reduction*, *50*, 101746. https://doi.org/10.1016/j.ijdrr.2020.101746

Kisiliuk, E., Leonenko, I., Khutorianskyi, O., Svoboda, I., & Banchuk-Petrosova, O. (2024). Regulation of Resource Management for Territorial Defense in the Context of Domestic and International Crime: International Legal Experience. *Pakistan Journal of Criminology*, *16*(3), 1333–1348. https://doi.org/10.62271/pjc.16.3.1333.1348

Kleider, H., & Toubeau, S. (2022). Public policy in multi-level systems: A new research agenda for the study of regional-level policy. *Regional and Federal Studies*, *32*(3), 277–305. https://doi.org/10.1080/13597566.2021.2018681

Kosal, M. (2024). How COVID-19 is reshaping U.S. national security policy. *Politics and the Life Sciences*, *43*(1), 83–98. https://doi.org/10.1017/pls.2023.13

Kwak, S. (2024). Dynamics between national security laws and repertoires of political action: A comparative analysis of Hong Kong and South Korea. *Asian Politics and Policy*, *16*(1), 78–93.

https://doi.org/10.1111/aspp.12725

Landauer, M., Skopik, F., Stojanović, B., Flatscher, A., & Ullrich, T. (2025). A review of time-series analysis for cyber security analytics: from intrusion detection to attack prediction. In *International Journal of Information Security* (Vol. 24, Issue 1). https://doi.org/10.1007/s10207-024-00921-0

Lebid, A. E., Stepanov, V. V., & Nazarov, M. S. (2023). The Informational Components of Social Resilience Within Realization of the UN Sustainable Development Goals. *International Journal of Media and Information Literacy*, *8*(2), 324–338. https://doi.org/10.13187/IJMIL.2023.2.324

Lee, J. (2023). "Not Time to Make a Change"? Reviewing the Rhetoric of Law Reform. *Current Legal Problems*, *76*(1), 129–172. https://doi.org/10.1093/clp/cuad004

Losada-Agudelo, M., & Souyris, S. (2024). Sustainable Operations Management in the Energy Sector: A Comprehensive Review of the Literature from 2000 to 2024. *Sustainability (Switzerland)*, *16*(18). https://doi.org/10.3390/su16187999

Lundberg, A., & Rova, E. (2022). Management Reforms in the Defence Sector. *Defence and Peace Economics*, *33*(4), 454–474. https://doi.org/10.1080/10242694.2021.1888014

Meislová, M. B., & Glencross, A. (2023). From multilateralism to bilateralism: Making sense of the UK's security cooperation with EU member states after 2016. *British Journal of Politics and International Relations*, *X*. https://doi.org/10.1177/13691481231208146

Metawe, M. (2024). Populism and domestic/international politics: theory and practice. *Review of Economics and Political Science*, *9*(3), 194–211. https://doi.org/10.1108/REPS-11-2019-0146

Ofte, H. J., & Katsikas, S. (2023). Understanding situation awareness in SOCs, a systematic literature review. *Computers and Security*, *126*. https://doi.org/10.1016/j.cose.2022.103069

Peck, J., Meulbroek, C., & Anguelov, D. (2024). Hong Kong's new normal: Remaking authorized discourses of "special administration," 2017–2022. *Environment and Planning C: Politics and Space*. https://doi.org/10.1177/23996544241227159

Rashed, M., Alneyadi, M. A. H., & Normalini, M. K. (2025). *Intelligent Protection: A Study Of The Key Drivers Of Intention To Adopt Artificial Intelligence (AI) Cybersecurity Systems In The UAE*. *20*. https://doi.org/https://doi.org/10.28945/5430

Sahoo, S., Dragicevic, T., & Blaabjerg, F. (2021). Cyber security in control of grid-tied power electronic converters - Challenges and vulnerabilities. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, *9*(5), 5326–5340. https://doi.org/10.1109/JESTPE.2019.2953480

Scott, P. F. (2024). 'State threats', security, and democracy: the National Security Act 2023. *Legal Studies*, *44*(2), 260–276. https://doi.org/10.1017/lst.2023.39

Seo, S., Moon, H., Lee, S., Kim, D., Lee, J., Kim, B., Lee, W., & Kim, D. (2023). D3GF: A Study on Optimal Defense Performance Evaluation of Drone-Type Moving Target Defense Through Game Theory. *IEEE Access*, *11*(April), 59575–59598. https://doi.org/10.1109/ACCESS.2023.3278744

Shkuta, O., Leheza, Y., Telelym, I., Anosienkov, A., & Yaroshak, O. (2024). National Security in the Conditions of the Russia-Ukraine War: Legal Regulation and Islamic Law Perspectives. *Al-Ahkam*, *34*(1), 99–120. https://doi.org/10.21580/ahkam.2024.34.1.20413

Suchkov, M. A. (2021). Whose hybrid warfare? How 'the hybrid warfare' concept shapes Russian discourse, military, and political practice. *Small Wars and Insurgencies*, *32*(3), 415–440. https://doi.org/10.1080/09592318.2021.1887434

Sydorchuk, O., Bashtannyk, V., Terkhanov, F., Kravtsov, O., Akimova, L., & Akimov, O. (2024). Integrating digitization into public administration: Impact on national security and the economy through spatial planning. *Edelweiss Applied Science and Technology*, *8*(5), 747–759. https://doi.org/10.55214/25768484.v8i5.1740

Tin, D., Barten, D. G., Granholm, F., Kovtonyuk, P., Burkle, F. M., & Ciottone, G. R. (2023). Hybrid warfare and counter-terrorism medicine. *European Journal of Trauma and Emergency Surgery*, *49*(2), 589–593. https://doi.org/10.1007/s00068-023-02230-y

Tušer, I., Jánský, J., & Petráš, A. (2021). Assessment of military preparedness for naturogenic threat: the COVID-19 pandemic in the Czech Republic. *Heliyon*, *7*(4). https://doi.org/10.1016/j.heliyon.2021.e06817

Tyulenev, S. (2021). Translation and (counter-)intelligence: the interpenetration of social-systemic boundary phenomena. *Perspectives: Studies in Translation Theory and Practice*, *29*(3), 339–353. https://doi.org/10.1080/0907676X.2020.1726977

Yamin, M. M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications*, *57*(January), 102722. https://doi.org/10.1016/j.jisa.2020.102722

Yanchenko, K., Shestopalova, A., von Nordheim, G., & Kleinen-von Königslöw, K. (2024). "Repressed

Opposition Media" or "Tools of Hybrid Warfare"? Negotiating the Boundaries of Legitimate Journalism in Ukraine Prior to Russia's Full-Scale Invasion. *International Journal of Press/Politics*, *29*(2), 351–370. https://doi.org/10.1177/19401612231167791

Zhang, C. (2024). Energy governance in China: A mixture of democratic environmentalism and authoritarian environmentalism. *Environmental Policy and Governance*, *34*(4), 352–362. https://doi.org/10.1002/eet.2089