Diversity UIKA Bogor
E-ISSN: 2776-9798

Diversity
JURNAL ILMIAH PASCASARJANA

http://ejournal.uika-bogor.ac.id/index.php/diversity

Pergeseran Paradigma dalam Perumusan dan Implementasi Kebijakan Pertahanan

Aris Sarjito[a*]
[a]*Universitas Pertahanan Republik Indonesia, Indonesia*
** Corresponding author e-mail: arissarjito@gmail.com*

DOI : 10.32832/djip-uika.v14i2.16812

ABSTRAK

Dalam beberapa tahun terakhir, kebijakan pertahanan di seluruh dunia telah mengalami transformasi yang signifikan karena kemajuan teknologi, pergeseran dinamika geopolitik, dan munculnya ancaman asimetris. Penelitian ini bertujuan untuk mengeksplorasi pergeseran paradigma dalam perumusan dan implementasi kebijakan pertahanan, dengan fokus pada tiga bidang utama: pengaruh kemajuan teknologi, dampak dari perubahan dinamika geopolitik, dan efektivitas kebijakan saat ini dalam melawan ancaman asimetris. Memanfaatkan metode penelitian kualitatif, termasuk studi kasus dan analisis kebijakan, penelitian ini meneliti bagaimana teknologi yang muncul seperti kecerdasan buatan dan sistem tak berawak diintegrasikan ke dalam strategi pertahanan. Ini juga menilai bagaimana munculnya kekuatan global baru dan konflik regional telah mendorong penyesuaian strategis oleh kekuatan besar dan aliansi, seperti AS, Cina, dan NATO. Selain itu, penelitian ini mengevaluasi kecukupan kebijakan yang ada dalam menangani perang siber, perang hibrida, dan terorisme. Temuan menunjukkan bahwa sementara kemajuan teknologi dan pergeseran geopolitik telah mendorong perubahan substansial dalam kebijakan pertahanan, tantangan tetap dalam mencapai koordinasi antar-lembaga yang efektif, beradaptasi dengan perubahan teknologi yang cepat, dan menangani akar penyebab terorisme. Studi ini menyimpulkan bahwa adaptasi dan inovasi berkelanjutan dalam strategi pertahanan sangat penting untuk menjaga keamanan dan stabilitas dalam lanskap global yang semakin kompleks.

Kata kunci: ancaman asimetris; dinamika geopolitik; kebijakan pertahanan; kemajuan teknologi; perang siber

Paradigm Shift in Defense Policy Formulation and Implementation

ABSTRACT

In recent years, defense policies worldwide have undergone significant transformations due to technological advancements, shifting geopolitical dynamics, and the rise of asymmetric threats. This research aims to explore the paradigm shift in defense policy formulation and implementation, focusing on three key areas: the influence of technological advancements, the impact of changing geopolitical dynamics, and the effectiveness of current policies in countering asymmetric threats. Utilizing qualitative research methods, including case studies and policy analysis, this study examines how emerging technologies like artificial intelligence and unmanned systems are integrated into defense strategies. It also assesses how the rise of new global powers and regional conflicts have prompted strategic adjustments by major powers and alliances, such as the U.S., China, and NATO. Additionally, the research evaluates the adequacy of existing policies in addressing cyber warfare, hybrid warfare, and terrorism. Findings indicate that while

technological advancements and geopolitical shifts have driven substantial changes in defense policies, challenges remain in achieving effective inter-agency coordination, adapting to rapid technological changes, and addressing the root causes of terrorism. The study concludes that continuous adaptation and innovation in defense strategies are essential for maintaining security and stability in an increasingly complex global landscape.

Keywords: *asymmetric threats; cyber warfare; defense policy; geopolitical dynamics; technological advancements*

PENDAHULUAN

Konvergensi kemajuan teknologi, pergeseran geopolitik, dan tantangan keamanan yang muncul mengkatalisasi transformasi signifikan dalam bidang pengembangan dan pelaksanaan kebijakan pertahanan. Penelitian ini menggali pergeseran paradigma dalam kebijakan pertahanan, menggarisbawahi studi terbaru dan kemajuan yang menggarisbawahi karakter yang berkembang dari strategi keamanan nasional dan global.

Salah satu pendorong perubahan paling signifikan dalam kebijakan pertahanan adalah kemajuan teknologi yang pesat. Teknologi baru seperti *Artificial Intelligence* (AI), kemampuan siber, dan sistem tak berawak membentuk kembali strategi dan operasi militer. Integrasi AI ke dalam mekanisme pertahanan, misalnya, meningkatkan proses pengambilan keputusan dan efisiensi operasional. Menurut sebuah studi oleh RAND Corporation, aplikasi AI dalam pertahanan berkisar dari pemeliharaan prediktif peralatan militer hingga sistem otonom yang mampu melakukan misi kompleks tanpa campur tangan manusia (Libicki, 2020).

Keamanan siber juga telah menjadi landasan kebijakan pertahanan modern. Meningkatnya frekuensi dan kecanggihan serangan siber memerlukan strategi keamanan siber yang kuat untuk melindungi infrastruktur penting dan informasi sensitif. Laporan oleh International Institute for Strategic Studies (IISS) menyoroti bahwa negara-negara sekarang memprioritaskan kemampuan pertahanan siber, dengan investasi signifikan dalam kerangka kerja keamanan siber dan pembentukan komando siber khusus (International Institute for Strategic Studies (IISS), 2021).

Pergeseran geopolitik adalah faktor penting lainnya yang mempengaruhi kebijakan pertahanan. Munculnya kekuatan global baru dan munculnya kembali persaingan kekuatan besar telah mendorong negara-negara untuk menilai kembali strategi pertahanan mereka. Persaingan strategis antara Amerika Serikat dan Tiongkok, misalnya, telah menyebabkan peningkatan fokus pada kawasan Indo-Pasifik. Sebuah studi oleh Center for a New American Security (CNAS) mencatat bahwa

A.S. meningkatkan kehadiran dan aliansi militernya di Indo-Pasifik untuk mengimbangi pengaruh Tiongkok yang semakin besar (Ratner, 2021).

Selain itu, aliansi NATO mengadaptasi strateginya untuk mengatasi ancaman dari aktor negara dan non-negara. Perkembangan terakhir di Eropa Timur, khususnya konflik di Ukraina, telah menggarisbawahi perlunya NATO untuk meningkatkan pencegahan dan postur pertahanannya. Penelitian Dewan Atlantik menunjukkan bahwa NATO berinvestasi dalam pasukan respons cepat dan meningkatkan latihan militernya untuk memastikan kesiapan melawan potensi agresi (Breedlove & Scaparrotti, 2022).

Sifat ancaman keamanan telah berkembang, mengharuskan pergeseran dalam perumusan kebijakan pertahanan. Ancaman militer tradisional sekarang dilengkapi dengan ancaman asimetris seperti terorisme, perang hibrida, dan *proliferasi weapons of mass destruction* (WMDs). Kompleksitas ancaman ini membutuhkan pendekatan pertahanan yang komprehensif dan multidimensi.

Perang hibrida, yang menggabungkan taktik militer konvensional dengan taktik tidak teratur dan perang siber, menimbulkan tantangan yang signifikan. Konflik di Ukraina telah mencontohkan penggunaan perang hibrida, di mana kekuatan konvensional, serangan siber, dan perang informasi digunakan secara bersamaan. Penelitian oleh European Council on Foreign Relations (ECFR) menunjukkan bahwa melawan ancaman hibrida membutuhkan tanggapan sipil dan militer yang terintegrasi, serta kerja sama internasional (Liik, 2021).

Terorisme tetap menjadi ancaman terus-menerus, dengan aktor non-negara mengeksploitasi kemajuan teknologi dan jaringan global. Kebijakan pertahanan semakin berfokus pada langkah-langkah kontra-terorisme yang mencakup berbagi intelijen, kolaborasi internasional, dan mengatasi akar penyebab terorisme. Laporan Global Terrorism Index 2022 menekankan pentingnya mengadopsi pendekatan holistik yang mencakup pembangunan sosial-ekonomi, program kontra-radikalisasi, dan meningkatkan kemampuan penegakan hukum (Institute for Economics and Peace, 2022).

Pergeseran paradigma dalam perumusan dan implementasi kebijakan pertahanan ditandai dengan integrasi teknologi canggih, adaptasi terhadap dinamika geopolitik, dan respons terhadap ancaman keamanan yang berkembang. Penelitian terbaru menggarisbawahi pentingnya ketangkasan dan inovasi dalam strategi pertahanan untuk mengatasi kompleksitas tantangan keamanan modern. Ketika negara-negara terus menavigasi lanskap transformatif ini, penekanan pada integrasi teknologi,

aliansi strategis, dan mitigasi ancaman komprehensif akan sangat penting dalam membentuk kebijakan pertahanan yang efektif untuk masa depan.

Dalam beberapa tahun terakhir, kemajuan teknologi yang pesat, ketegangan geopolitik yang berkembang, dan ancaman asimetris yang muncul telah secara drastis mengubah lanskap kebijakan pertahanan global. Strategi tradisional yang berpusat pada kemampuan militer konvensional terbukti tidak memadai dalam menghadapi tantangan keamanan modern. Negara-negara dengan demikian dipaksa untuk menilai kembali dan membentuk kembali kebijakan pertahanan mereka untuk memasukkan teknologi baru, menyesuaikan diri dengan dinamika geopolitik yang bergeser, dan dengan mahir melawan ancaman non-tradisional seperti perang siber, perang hibrida, dan terorisme. Pergeseran paradigma ini menggarisbawahi perlunya pemahaman menyeluruh tentang pendorong di balik transformasi ini dan implikasinya yang mendalam bagi keamanan nasional dan stabilitas internasional.

Penelitian ini bertujuan untuk menganalisis pengaruh kemajuan teknologi terhadap perumusan dan implementasi kebijakan pertahanan, menguji pengaruh dinamika geopolitik terhadap strategi pertahanan nasional dan internasional, dan mengevaluasi efektivitas kebijakan pertahanan saat ini dalam mengatasi ancaman asimetris.

Pertanyaan penelitian untuk penelitian ini mencakup mengeksplorasi dampak transformatif dari kemajuan teknologi pada kebijakan pertahanan, khususnya dalam mengintegrasikan kecerdasan buatan, keamanan siber, dan sistem tak berawak untuk meningkatkan kemampuan operasional dan pengambilan keputusan (Libicki, 2020). Selain itu, laporan ini menyelidiki bagaimana dinamika geopolitik yang berkembang, seperti munculnya kekuatan global baru dan konflik regional, mempengaruhi strategi pertahanan nasional dan internasional, dengan fokus pada adaptasi oleh kekuatan besar dan aliansi seperti A.S., Tiongkok, dan NATO untuk menjaga keamanan di tengah pergeseran ini (Breedlove & Scaparrotti, 2022; Ratner, 2021). Selain itu, studi ini menilai efektivitas kebijakan pertahanan saat ini dalam mengatasi ancaman asimetris, termasuk perang siber, perang hibrida, dan terorisme, mengevaluasi strategi yang digunakan dan mengusulkan peningkatan ketahanan kebijakan dan kemampuan beradaptasi dalam menanggapi tantangan yang kompleks dan berkembang ini (Institute for Economics and Peace, 2022; Liik, 2021).

METODE PENELITIAN

Metode penelitian kualitatif sangat penting untuk mengeksplorasi fenomena kompleks seperti pergeseran paradigma dalam perumusan dan implementasi kebijakan pertahanan. Penelitian ini menggali penggunaan data sekunder dalam penelitian kualitatif, menggambar pada kerangka kerja dan pedoman yang disediakan oleh John W. Creswell. Ini menyoroti penerapan metode ini untuk memahami nuansa kebijakan pertahanan modern yang didorong oleh perubahan teknologi, geopolitik, dan terkait keamanan.

John W. Creswell, seorang tokoh terkemuka dalam penelitian kualitatif, menggarisbawahi pentingnya pemahaman kontekstual dan makna dalam fenomena sosial. Menurut Creswell (2014), Penelitian kualitatif menggali makna yang dikaitkan oleh individu atau kelompok dengan masalah sosial atau manusia, sehingga ideal untuk mengeksplorasi isu-isu kompleks seperti pergeseran kebijakan pertahanan. Pendekatan ini memungkinkan eksplorasi mendalam tentang beragam faktor yang mempengaruhi dan perspektif pemangku kepentingan, penting untuk menganalisis secara komprehensif nuansa strategi pertahanan kontemporer dan implikasinya.

Data sekunder, sebagaimana didefinisikan oleh Creswell, (2014), terdiri dari informasi yang dikumpulkan oleh peneliti atau lembaga lain untuk tujuan yang tidak terkait dengan penelitian saat ini. Jenis data ini sangat berharga dalam penelitian kualitatif, memberikan wawasan kontekstual yang mendalam tanpa perlu pengumpulan data primer. Dalam konteks mempelajari perubahan paradigma dalam kebijakan pertahanan, sumber data sekunder mencakup beragam bahan seperti laporan pemerintah, dokumen kebijakan, publikasi akademik, artikel berita, dan catatan sejarah. Sumber-sumber ini tidak hanya memperkaya pemahaman tentang strategi pertahanan yang berkembang tetapi juga memfasilitasi analisis komprehensif tentang faktor-faktor yang mempengaruhi perumusan dan implementasi kebijakan dari waktu ke waktu.

Dalam penelitian kebijakan pertahanan, metode data sekunder seperti analisis dokumen, analisis konten, dan analisis historis memainkan peran penting dalam mengungkap wawasan dan tren. Analisis dokumen, seperti yang dijelaskan oleh Creswell (2014), melibatkan peninjauan secara sistematis berbagai dokumen—mulai dari kertas kebijakan hingga laporan militer—untuk memahami evolusi strategi pertahanan dalam menanggapi ancaman yang muncul dan pergeseran geopolitik (Breedlove & Scaparrotti, 2022). Demikian pula, analisis konten memungkinkan para peneliti untuk mengukur dan menafsirkan tema dalam data

kualitatif, seperti laporan media tentang insiden perang siber yang mencerminkan meningkatnya penekanan pada keamanan siber dalam strategi pertahanan nasional (International Institute for Strategic Studies (IISS), 2021). Analisis historis melengkapi metode ini dengan memberikan konteks dari peristiwa masa lalu, menawarkan pelajaran yang menginformasikan keputusan kebijakan masa kini, seperti penyesuaian strategis yang dibuat oleh aliansi militer seperti NATO dalam menanggapi tantangan kontemporer (Ratner, 2021). Sementara data sekunder menawarkan akses hemat biaya ke informasi yang luas, peneliti harus menavigasi pertimbangan etis, memastikan akurasi data dan menjaga terhadap bias dalam topik sensitif seperti kebijakan pertahanan. Kemampuan beradaptasi dalam kerangka kerja analitis sangat penting untuk secara efektif memanfaatkan data yang tersedia sambil mempertahankan standar metodologis yang ketat.

Metode penelitian kualitatif menggunakan data sekunder, sebagaimana diuraikan oleh John W. Creswell, memberikan kerangka kerja yang kuat untuk mengeksplorasi perubahan paradigma dalam perumusan dan implementasi kebijakan pertahanan. Melalui analisis dokumen, analisis konten, dan analisis historis, peneliti dapat memperoleh wawasan komprehensif tentang faktor-faktor yang mendorong perubahan dalam kebijakan pertahanan dan implikasinya. Dengan memanfaatkan sumber data sekunder yang kredibel dan relevan, para peneliti dapat berkontribusi pada pemahaman yang lebih dalam tentang bagaimana negara-negara mengadaptasi strategi pertahanan mereka dalam menghadapi kemajuan teknologi, dinamika geopolitik, dan ancaman keamanan yang berkembang.

HASIL DAN PEMBAHASAN

Kemajuan teknologi telah secara signifikan mempengaruhi perumusan dan implementasi kebijakan pertahanan, membentuk kembali strategi militer, kemampuan operasional, dan proses pengambilan keputusan. Teknologi baru seperti *Artificial Intelligence* (AI), keamanan siber, dan sistem tak berawak sangat penting dalam strategi pertahanan modern, meningkatkan efektivitas militer dan perencanaan strategis. Memeriksa studi kasus dan inisiatif pertahanan baru-baru ini menyoroti dampak transformatif dari teknologi ini pada operasi militer kontemporer (Johnson, 2019).

Artificial Intelligence (AI) memainkan peran penting dalam membentuk kebijakan pertahanan dengan meningkatkan berbagai operasi militer, termasuk analisis intelijen dan sistem senjata otonom. Kemampuan AI untuk memproses dan menganalisis volume data yang besar secara *real-time* telah merevolusi kemampuan *Intelligence, Surveillance, and Reconnaissance* (ISR), memungkinkan identifikasi

pola dan anomali yang mungkin terlewatkan oleh analis manusia, sehingga secara signifikan meningkatkan kesadaran situasional dan pengambilan keputusan (Abaimov & Martellini, 2020; Libicki, 2020).

Salah satu studi kasus penting adalah Proyek Maven Departemen Pertahanan Amerika Serikat, yang menggunakan AI untuk menganalisis rekaman video dari drone. Project Maven telah menunjukkan potensi AI untuk mempercepat pemrosesan data dan meningkatkan akurasi identifikasi target, sehingga meningkatkan efisiensi operasional dan mengurangi beban kognitif pada analis manusia (Sayler, 2020).

AI juga memainkan peran penting dalam pemeliharaan prediktif, yang membantu menjaga kesiapan peralatan militer. Dengan memprediksi kegagalan peralatan sebelum terjadi, pemeliharaan prediktif berbasis AI dapat mengurangi waktu henti dan biaya pemeliharaan, memastikan bahwa aset militer selalu siap tempur. Aplikasi AI ini telah diterapkan di berbagai cabang militer AS, termasuk penggunaan AI oleh Angkatan Udara untuk memprediksi kebutuhan perawatan pesawat (Defense Innovation Board, 2019).

Keamanan siber adalah landasan kebijakan pertahanan modern, didorong oleh frekuensi dan kecanggihan serangan siber yang terus meningkat. Strategi pertahanan kontemporer memprioritaskan perlindungan infrastruktur penting, jaringan militer, dan informasi sensitif dari ancaman siber. Pembentukan komando siber khusus, seperti Komando Siber A.S. dan entitas serupa di seluruh dunia, menggarisbawahi peran penting keamanan siber dalam pertahanan nasional (Naseer, 2020).

Prakarsa pertahanan baru-baru ini menyoroti integrasi keamanan siber ke dalam strategi pertahanan yang lebih luas. Misalnya, NATO telah mengakui dunia maya sebagai domain operasi, di samping darat, laut, udara, dan ruang angkasa. Pengakuan ini telah mengarah pada pengembangan kebijakan pertahanan siber yang komprehensif, termasuk peningkatan kemampuan siber negara-negara anggota dan pembentukan tim respons cepat untuk melawan ancaman siber (NATO, 2020).

Studi kasus insiden dunia maya, seperti serangan *ransomware* WannaCry 2017 dan peretasan SolarWinds 2020, menggambarkan kebutuhan kritis akan langkah-langkah keamanan siber yang kuat. Insiden ini telah mendorong pemerintah untuk berinvestasi dalam teknologi pertahanan siber canggih dan mengembangkan kerangka kerja kolaboratif untuk berbagi informasi dan operasi siber bersama (Sanger, 2019; Zetter, 2015).

Sistem tak berawak, seperti *drone* dan kendaraan otonom, telah berdampak signifikan terhadap kebijakan pertahanan dengan meningkatkan fleksibilitas operasional dan mengurangi risiko terhadap personel manusia. *Drone*, khususnya, telah menjadi sangat diperlukan untuk misi intelijen, pengawasan, dan pengintaian (ISR), serangan presisi, dan dukungan logistik, sehingga mengubah operasi militer modern.

Penggunaan *drone* untuk serangan presisi telah menjadi *game-changer* dalam operasi kontra-terorisme. Misalnya, penggunaan *drone* oleh militer AS untuk menargetkan para pemimpin teroris bernilai tinggi di Timur Tengah telah menunjukkan efektivitas sistem tak berawak dalam melaksanakan serangan yang tepat dan kerusakan jaminan rendah. Kemampuan ini telah menyebabkan pergeseran dalam kebijakan pertahanan ke arah menggabungkan lebih banyak sistem tak berawak untuk operasi yang ditargetkan (Zenko, 2016).

Sistem tak berawak juga memainkan peran penting dalam pengawasan dan pengintaian. *Drone* yang dilengkapi dengan sensor dan kamera canggih dapat mengumpulkan intelijen di area yang sulit atau berbahaya bagi pesawat berawak untuk diakses. Kemampuan ini meningkatkan kesadaran situasional dan memberikan informasi *real-time* kepada komandan, memungkinkan pengambilan keputusan yang lebih tepat selama operasi militer (Singer, 2009).

Selanjutnya, kendaraan otonom sedang dikembangkan untuk melakukan berbagai peran pendukung, seperti logistik dan transportasi. Penggunaan konvoi otonom untuk mengirimkan pasokan di zona tempur mengurangi risiko bagi pengemudi manusia dan meningkatkan efisiensi operasi logistik. Program Autonomous Ground Resupply (AGR) Angkatan Darat AS adalah salah satu inisiatif yang bertujuan mengembangkan kendaraan otonom untuk dukungan logistik (U.S. Army, 2021).

Pergeseran lanskap geopolitik, ditandai dengan munculnya kekuatan global baru dan konflik regional, telah secara signifikan mempengaruhi strategi pertahanan nasional dan internasional. Dinamika geopolitik yang berkembang, khususnya di Indo-Pasifik dan Eropa Timur, membentuk kembali kebijakan pertahanan ketika kekuatan dan aliansi utama seperti Amerika Serikat, Tiongkok, dan NATO melakukan penyesuaian strategis untuk menjaga keamanan dan stabilitas di tengah tantangan yang muncul (Auslin, 2020).

Pertumbuhan ekonomi dan militer Tiongkok yang cepat telah secara fundamental mengubah dinamika geopolitik kawasan Indo-Pasifik. Melalui prakarsa seperti Belt and Road Initiative (BRI) dan tindakan tegas di Laut Cina Selatan, Tiongkok telah

memperluas pengaruhnya, mendorong kekuatan regional dan aktor global untuk memikirkan kembali strategi pertahanan mereka (Kapur, 2019).

Amerika Serikat, memandang China sebagai pesaing strategis, telah menerapkan beberapa langkah untuk mengimbangi pengaruh China. Strategi Indo-Pasifik A.S. menekankan penguatan aliansi dan kemitraan, meningkatkan kehadiran militer, dan mempromosikan Indo-Pasifik yang bebas dan terbuka (Hu & Meng, 2020). Strategi ini mencakup prakarsa seperti Dialog Keamanan Kuadrilateral (Quadrilateral Security Dialogue – Quad) yang melibatkan A.S., Jepang, India, dan Australia, yang bertujuan untuk mengoordinasikan upaya pertahanan dan memastikan stabilitas regional.

Jepang juga telah menyesuaikan kebijakan pertahanannya sebagai tanggapan atas kebangkitan China. Pedoman Program Pertahanan Nasional (National Defense Program Guidelines – NDPG) Jepang menggarisbawahi perlunya meningkatkan kemampuan pertahanan dan memperkuat aliansi A.S.-Jepang. Ini termasuk memperoleh teknologi canggih dan meningkatkan anggaran pertahanan untuk mengatasi potensi ancaman dari Tiongkok (Japan Ministry of Defense, 2020).

Strategi pertahanan Australia, yang diuraikan dalam Pembaruan Strategis Pertahanan 2020, menyoroti pentingnya kawasan Indo-Pasifik yang aman. Pembaruan itu menyerukan peningkatan pengeluaran pertahanan, modernisasi kemampuan militer, dan keterlibatan yang lebih dalam dengan mitra regional untuk mencegah agresi dan melindungi kepentingan nasional (Australian Department of Defence, 2020).

Eropa Timur telah menjadi titik fokus ketegangan geopolitik karena tindakan Rusia di Ukraina dan ambisi regionalnya yang lebih luas. Aneksasi Krimea pada tahun 2014 dan konflik yang sedang berlangsung di Ukraina Timur telah mendorong NATO dan negara-negara anggotanya untuk menilai kembali strategi pertahanan mereka (Moore & Coletta, 2017).

Tanggapan NATO telah ditandai dengan pergeseran ke arah pertahanan dan pencegahan kolektif. Inisiatif Enhanced Forward Presence (EFP) melibatkan penyebaran kelompok pertempuran multinasional di negara-negara Baltik dan Polandia untuk mencegah potensi agresi. NATO juga telah meningkatkan frekuensi dan skala latihan militernya untuk memastikan kesiapan dan menunjukkan komitmennya untuk membela negara-negara anggotanya (Luik & Praks, 2017).

Uni Eropa juga telah mengambil langkah-langkah untuk meningkatkan kemampuan pertahanannya melalui inisiatif seperti Permanent Structured Cooperation (PESCO)

dan European Defence Fund (EDF). Inisiatif ini bertujuan untuk meningkatkan kerja sama di antara negara-negara anggota UE, mengembangkan proyek pertahanan bersama, dan mengurangi ketergantungan pada aktor eksternal scurity (European Union External Action, 2021b).

Modernisasi militer Rusia dan kebijakan luar negeri yang tegas telah mengharuskan penyesuaian strategis oleh NATO dan negara-negara anggotanya. Menanggapi pengembangan sistem senjata canggih, kemampuan dunia maya, dan taktik perang hibrida Rusia, negara-negara NATO telah meningkatkan investasi pertahanan mereka. Misalnya, Inggris telah mengumumkan rencana untuk meningkatkan pengeluaran pertahanan dan mengembangkan kemampuan baru untuk melawan ancaman hibrida dan serangan siber (UK Ministry of Defence, 2021).

Ambisi strategis Tiongkok juga telah mendorong perubahan dalam strategi pertahanan di luar Indo-Pasifik. Misalnya China's Belt and Road Initiative meluas ke kawasan seperti Asia Tengah dan Eropa, mempengaruhi pertahanan dan kebijakan luar negeri negara-negara di sepanjang rute ini. Sebagai tanggapan, negara-negara meningkatkan kerja sama militer mereka dan mencari kemitraan keamanan baru untuk menyeimbangkan pengaruh China (Brzezinski & Xiang, 2021).

Dalam beberapa tahun terakhir, ancaman global telah berevolusi dari konflik negara-ke-negara tradisional untuk memasukkan ancaman asimetris seperti perang dunia maya, perang hibrida, dan terorisme. Diskusi ini menilai efektivitas kebijakan pertahanan saat ini dalam mengatasi ancaman non-tradisional ini dengan memeriksa strategi yang digunakan, kekuatan, dan kelemahannya. Dengan menganalisis insiden spesifik dan respons pertahanan, studi ini memberikan rekomendasi untuk meningkatkan ketahanan dan kemampuan beradaptasi kebijakan pertahanan untuk mengatasi ancaman yang kompleks dan beragam ini dengan lebih baik.

Perang siber telah menjadi masalah keamanan nasional yang kritis, dengan aktor negara dan non-negara semakin menggunakan serangan siber untuk mencapai tujuan strategis. Kompleksitas dan anonimitas operasi siber membuat mereka sangat menantang untuk dipertahankan. Sebagai tanggapan, kebijakan pertahanan saat ini berfokus pada pengembangan kerangka kerja keamanan siber yang kuat dan pembentukan unit pertahanan siber khusus (Relia, 2015).

Misalnya, Amerika Serikat mendirikan U.S. Cyber Command (USCYBERCOM) untuk mengoordinasikan dan meningkatkan kemampuan pertahanan sibernya. Inisiatif ini telah secara signifikan meningkatkan kemampuan negara untuk

mendeteksi dan menanggapi ancaman siber. Namun, insiden profil tinggi seperti peretasan SolarWinds pada tahun 2020 menyoroti kerentanan terus-menerus dalam infrastruktur dan rantai pasokan penting (Reeder & Hall, 2021). Meskipun ada investasi besar dalam keamanan siber, kesenjangan tetap ada dalam koordinasi antar-lembaga dan berbagi intelijen ancaman secara *real-time.*

NATO juga memprioritaskan pertahanan siber, mengakui dunia maya sebagai domain operasi. Pembentukan NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) dan pengembangan kebijakan pertahanan siber yang komprehensif telah memperkuat postur pertahanan siber kolektif aliansi tersebut. Meskipun demikian, laju perubahan teknologi yang cepat dan proliferasi ancaman siber yang canggih memerlukan adaptasi dan investasi berkelanjutan dalam langkah-langkah keamanan siber (NATO, 2020).

Perang hibrida, yang memadukan operasi militer konvensional dengan taktik tidak teratur, aktivitas siber, dan perang informasi, menimbulkan tantangan signifikan terhadap strategi pertahanan tradisional. Tindakan Rusia di Krimea dan Ukraina Timur mencontohkan bagaimana perang hibrida dapat secara efektif mencapai tujuan strategis sambil mempertahankan penyangkalan yang masuk akal (Fabian, 2019).

Kebijakan pertahanan saat ini telah berjuang untuk secara efektif melawan ancaman hibrida karena sifatnya yang beragam. Peningkatan kehadiran NATO di Eropa Timur dan peningkatan latihan militer adalah langkah-langkah menuju penanganan aspek konvensional perang hibrida. Namun, melawan elemen non-konvensional, seperti kampanye disinformasi dan serangan siber, membutuhkan pendekatan yang lebih terintegrasi dan fleksibel (Anagnostakis, 2023).

Upaya Uni Eropa untuk memerangi ancaman hibrida melalui inisiatif seperti European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) patut dipuji. Inisiatif ini bertujuan untuk meningkatkan ketahanan dan meningkatkan kerja sama di antara negara-negara anggota. Terlepas dari upaya ini, UE menghadapi tantangan dalam mencapai respons terpadu dan terkoordinasi karena berbagai tingkat kesiapan dan prioritas nasional yang berbeda (European Union External Action, 2021a).

Terorisme tetap menjadi ancaman terus-menerus, dengan organisasi teroris terus mengadaptasi taktik mereka dan mengeksploitasi teknologi baru. Untuk memerangi terorisme, kebijakan pertahanan telah difokuskan pada kombinasi operasi militer, pengumpulan intelijen, dan upaya kontra-radikalisasi (Schnader, 2019).

Perang Global Melawan Teror AS, yang diluncurkan setelah serangan 11 September, telah menyebabkan penghapusan para pemimpin teroris utama dan gangguan jaringan teroris. Namun, munculnya kelompok teroris yang terdesentralisasi dan penyerang tunggal menghadirkan tantangan baru. Kemampuan kelompok-kelompok seperti ISIS untuk menginspirasi dan mengarahkan serangan melalui propaganda Online menggarisbawahi perlunya strategi kontra-radikalisasi yang efektif (Byman, 2019).

Negara-negara Eropa telah menerapkan berbagai langkah untuk mengatasi ancaman terorisme, termasuk peningkatan keamanan perbatasan, peningkatan pembagian intelijen, dan operasi kontra-terorisme. Pembentukan European Counter Terrorism Centre (ECTC) dalam Europol telah meningkatkan koordinasi di antara negara-negara anggota. Namun demikian, ancaman terorisme yang tumbuh di dalam negeri dan radikalisasi individu di Eropa menyoroti perlunya pendekatan yang lebih komprehensif yang mengatasi akar penyebab terorisme (European Commission, 2020).

Kebijakan pertahanan saat ini menunjukkan beberapa kekuatan dalam mengatasi ancaman asimetris, seperti pembentukan unit dan pusat khusus, peningkatan kerja sama internasional, dan pengembangan kerangka kerja komprehensif, yang telah meningkatkan kemampuan untuk menanggapi perang siber, perang hibrida, dan terorisme. Namun, kelemahan signifikan tetap ada (Sarjito, 2023).

Salah satu kelemahan utama adalah sifat tertutup dari banyak kebijakan pertahanan, yang dapat menghambat koordinasi dan berbagi informasi yang efektif. Sifat ancaman asimetris yang dinamis dan saling berhubungan membutuhkan pendekatan yang lebih terintegrasi dan gesit. Selain itu, evolusi yang cepat dari ancaman ini memerlukan adaptasi dan inovasi berkelanjutan dalam strategi pertahanan (Nicander, 2015).

Untuk meningkatkan efektivitas kebijakan pertahanan dalam mengatasi ancaman asimetris, beberapa rekomendasi dapat dibuat: meningkatkan koordinasi dan berbagi informasi di antara lembaga pemerintah dan mitra internasional melalui satuan tugas bersama dan pusat komando terintegrasi; berinvestasi dalam teknologi mutakhir seperti kecerdasan buatan, pembelajaran mesin, dan komputasi kuantum untuk tetap berada di depan ancaman dunia maya yang muncul dan meningkatkan kemampuan prediktif; mengembangkan dan melaksanakan program kontra-radikalisasi komprehensif yang mengatasi akar penyebab terorisme, termasuk faktor sosial, ekonomi, dan ideologis; dan mengadopsi strategi fleksibel dan adaptif yang melibatkan tinjauan rutin dan pembaruan strategi pertahanan, yang diinformasikan oleh intelijen ancaman dan kemajuan teknologi terbaru.

KESIMPULAN

Kemajuan teknologi, khususnya dalam AI, keamanan siber, dan sistem tak berawak, telah secara signifikan mempengaruhi perumusan dan implementasi kebijakan pertahanan modern. Teknologi ini meningkatkan kemampuan operasional, meningkatkan proses pengambilan keputusan, dan menyediakan alat baru untuk mengatasi tantangan keamanan kontemporer. Dengan mengintegrasikan teknologi yang muncul ini ke dalam strategi pertahanan, organisasi militer dapat mempertahankan keunggulan strategis dan secara efektif menanggapi ancaman yang berkembang. Pengembangan dan implementasi berkelanjutan dari teknologi ini kemungkinan akan membentuk masa depan kebijakan pertahanan, mendorong inovasi dan transformasi lebih lanjut dalam operasi militer.

Dinamika geopolitik yang berkembang, didorong oleh munculnya kekuatan global baru dan konflik regional, telah secara signifikan mempengaruhi strategi pertahanan nasional dan internasional. Kebangkitan Tiongkok telah membentuk kembali kebijakan pertahanan di Indo-Pasifik, dengan Amerika Serikat dan sekutunya meningkatkan kehadiran dan kerja sama militer mereka untuk mengimbangi pengaruh Tiongkok. Di Eropa Timur, penyesuaian strategis NATO dalam menanggapi tindakan Rusia telah berfokus pada pertahanan dan pencegahan kolektif. Ketika lanskap geopolitik terus bergeser, negara-negara dan aliansi harus menyesuaikan strategi pertahanan mereka untuk mengatasi tantangan yang muncul dan menjaga keamanan dan stabilitas.

Kebijakan pertahanan saat ini telah membuat langkah signifikan dalam mengatasi ancaman asimetris seperti perang siber, perang hibrida, dan terorisme. Namun, sifat ancaman yang berkembang ini membutuhkan adaptasi dan perbaikan berkelanjutan. Dengan meningkatkan koordinasi, berinvestasi dalam teknologi canggih, menerapkan program kontra-radikalisasi yang komprehensif, dan mengadopsi strategi yang fleksibel, kebijakan pertahanan dapat menjadi lebih tangguh dan efektif dalam menjaga keamanan nasional dan internasional.

REFERENSI

Abaimov, S., & Martellini, M. (2020). Artificial intelligence in autonomous weapon systems. *21st Century Prometheus: Managing CBRN Safety and Security Affected by Cutting-Edge Technologies*, 141–177.

Anagnostakis, D. (2023). Hybrid Threats: A European Response. In *Handbook for Management of Threats: Security and Defense, Resilience and Optimal Strategies* (pp. 425–441). Springer.

Auslin, M. R. (2020). *Asia's new geopolitics: Essays on reshaping the Indo-Pacific*. Hoover Press.

Australian Department of Defence. (2020). *2020 Defence Strategic Update.*

Breedlove, P., & Scaparrotti, C. (2022). *Enhancing NATO's Deterrence and Defense Posture*. Atlantic Council.

Brzezinski, I., & Xiang, L. (2021). The Belt and Road Initiative and Its Impact on Global Securit. *Center for Strategic and International Studies*.

Byman, D. (2019). *Road warriors: Foreign fighters in the armies of jihad*. Oxford University Press.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.

Defense Innovation Board. (2019). AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense. *Defense Innovation Board*.

European Commission. (2020). *Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*.

European Union External Action. (2021a). *European Centre of Excellence for Countering Hybrid Threats*.

European Union External Action. (2021b). *Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF)*.

Fabian, S. (2019). The Russian hybrid warfare strategy–neither Russian nor strategy. *Defense & Security Analysis*, *35*(3), 308–325.

Hu, W., & Meng, W. (2020). The US Indo-Pacific strategy and China's response. *China Review*, *20*(3), 143–176.

Institute for Economics and Peace. (2022). *). Global Terrorism Index 2022*. Institute for Economics and Peace.

International Institute for Strategic Studies (IISS). (2021).). Cyber Capabilities and National Power: A Net Assessment. *International Institute for Strategic Studies (IISS)*.

Japan Ministry of Defense. (2020). *National Defense Program Guidelines for FY 2020 and Beyond*.

Johnson, J. (2019). Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis*, *35*(2), 147–169.

Kapur, A. (2019). *Geopolitics and the Indo-Pacific Region*. Routledge.

Libicki, M. C. (2020). *The Role of Artificial Intelligence in Military Decision-Making*. RAND Corporation.

Liik, K. (2021). *Countering Hybrid Threats in Europe: A Comprehensive Approach. European Council on Foreign Relations (ECFR)*.

Luik, J., & Praks, H. (2017). *Boosting the Deterrent Effect of Allied Enhanced Forward Presence*. International Centre for Defence and Security (ICDS).

Moore, R. R., & Coletta, D. V. (2017). *NATO's return to Europe: engaging Ukraine, Russia, and beyond*. Georgetown University Press.

Naseer, I. (2020). Cyber Defense for Data Protection and Enhancing Cyber Security Networks for Military and Government Organizations. *MZ Computing Journal*, *1*(1).

NATO. (2020). *Cyber Defence*.

Nicander, L. (2015). *New threats-old routines: bureaucratic adaptability in the security policy environment*.

Ratner, E. (2021). *Securing the Indo-Pacific: A Strategy for the United States and Its Allies*.

Reeder, J. R., & Hall, T. (2021). Cybersecurity's pearl harbor moment. *The Cyber Defense Review*, *6*(3), 15–40.

Relia, S. (2015). *Cyber warfare: its implications on national security*. Vij Books India Pvt Ltd.

Sanger, D. E. (2019). *The perfect weapon: War, sabotage, and fear in the cyber age*. Crown.

Sarjito, I. A. (2023). *Kebijakan dan Strategi Pertahanan*. CV Jejak (Jejak Publisher).

Sayler, K. M. (2020). Artificial intelligence and national security. *Congressional Research Service*, *45178*.

Schnader, J. (2019). The Implementation of Artificial Intelligence in Hard and Soft Counterterrorism Efforts on Social Media. *Santa Clara High Tech. LJ*, *36*, 42.

Singer, P. W. (2009). *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin.

UK Ministry of Defence. (2021). *Defence in a Competitive Age*.

U.S. Army. (2021). *Autonomous Ground Resupply*.

Zenko, M. (2016). *Drone Warfare*. Council on Foreign Relations.

Zetter, K. (2015). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown.