Jurnal Imu Sosial dan Ilmu Politik Universitas Jambi (JISIP-UNJA) Volume 8 Nomor 2 (2024) 149-158

BENCHMARK KEBIJAKAN PERTAHANAN NON MILITER DARI BERBAGAI NEGARA: SEBUAH REVIEW

Mohamad Kashuri [a]

[a] Deputi Bidang Pengawasan Obat Tradisional, Suplemen Kesehatan, dan Kosmetik, Badan Pengawas Obat dan Makanan, Jl. Percetakan Negara, No. 23, Jakarta Pusat, I0560, Indonesia
E-mail: mohamad.kashuri@pom.go.id

ABSTRAK

Dalam era globalisasi yang semakin kompleks, pertahanan non-militer telah menjadi komponen kritis dalam strategi keamanan nasional. Studi ini menganalisis dan membandingkan kebijakan pertahanan non-militer dari berbagai negara, termasuk Amerika Serikat, Cina, Rusia, Uni Eropa, Singapura, dan Australia, untuk mengidentifikasi praktik terbaik dan tren global. Fokus utama diberikan pada empat pilar pertahanan non-militer: diplomasi, ketahanan ekonomi, kesiapsiagaan siber, dan ketahanan masyarakat. Melalui analisis komparatif dan tinjauan literatur komprehensif, penelitian ini mengungkapkan bahwa negara-negara semakin memprioritaskan pendekatan holistik dalam pertahanan non-militer, mengintegrasikan berbagai sektor pemerintah dan masyarakat. Temuan menunjukkan tren menuju peningkatan investasi dalam keamanan siber, penguatan kemitraan publik-swasta, dan pengembangan strategi komunikasi yang efektif untuk menghadapi ancaman informasi. Studi ini juga mengidentifikasi inovasi-inovasi penting, seperti penggunaan kecerdasan buatan dalam deteksi ancaman dan implementasi program ketahanan masyarakat yang komprehensif. Tantangan utama yang dihadapi termasuk koordinasi antar lembaga, adaptasi terhadap teknologi yang berkembang pesat, dan keseimbangan antara keamanan nasional dan hak-hak individu. Berdasarkan temuan ini, penelitian merekomendasikan peningkatan kolaborasi internasional dalam pertukaran informasi dan praktik terbaik, investasi berkelanjutan dalam pendidikan dan pelatihan tenaga kerja pertahanan non-militer, serta pengembangan kerangka kebijakan yang fleksibel untuk menghadapi ancaman yang terus berevolusi. Studi ini memberikan wawasan berharga bagi pembuat kebijakan dan peneliti dalam merancang dan mengimplementasikan strategi pertahanan non-militer yang efektif di era kontemporer.

Kata Kunci: Pertahanan Non-Militer, Kebijakan Pertahanan, Geopolitik.

***ABSTRACT* (11pt, bold, Italic)**

In an increasingly complex era of globalization, non-military defense has become a critical component of national security strategies. This study analyzes and compares non-military defense policies from various countries, including the United States, China, Russia, the European Union, Singapore, and Australia, to identify best practices and global trends. The primary focus is given to four pillars of non-military defense: diplomacy, economic resilience, cyber preparedness, and societal resilience. Through comparative analysis and comprehensive literature review, this research reveals that countries are increasingly prioritizing a holistic approach to non-military defense, integrating various government sectors and society. Findings indicate trends towards increased investment in cybersecurity, strengthening public-private partnerships, and developing effective communication strategies to address information threats. The study also identifies key innovations, such as the use of artificial intelligence in threat detection and the implementation of comprehensive societal resilience programs. Major challenges faced include inter-agency coordination, adaptation to rapidly evolving technologies, and balancing national security with individual rights. Based on these findings, the research recommends enhancing international collaboration in information exchange and best practices, sustained investment in education and training of non-military defense workforce, and development of flexible policy frameworks to address evolving threats. This study provides valuable insights for policymakers and researchers in designing and implementing effective non-military defense strategies in the contemporary era.

Keywords: ***Non-Military Defense, Defense Policy, Geopolitics.***

* Corresponding Author. Tel: Mohamad Kashuri
E-mail: mohamad.kashuri@pom.go.id

PENDAHULUAN

Dalam lanskap keamanan global yang semakin kompleks, konsep pertahanan nasional telah berkembang melampaui pendekatan militer tradisional. Pertahanan non-militer, yang mencakup berbagai strategi dan kebijakan untuk melindungi kepentingan nasional tanpa menggunakan kekuatan militer, telah menjadi komponen kritis dalam kerangka keamanan nasional yang komprehensif (Cavelty & Mauer, 2020). Evolusi ini didorong oleh berbagai faktor, termasuk perubahan karakteristik ancaman, kemajuan teknologi, dan pergeseran dinamika geopolitik global.

Pertahanan non-militer meliputi berbagai aspek, termasuk diplomasi, ketahanan ekonomi, keamanan siber, dan ketahanan masyarakat. Menurut Nye (2011), konsep "soft power" dan kemampuan untuk mempengaruhi perilaku negara lain tanpa paksaan telah menjadi semakin penting dalam hubungan internasional kontemporer. Sementara itu, Brooks dan Wohlforth (2016) menekankan pentingnya ketahanan ekonomi sebagai fondasi kekuatan nasional dalam sistem internasional yang saling tergantung.

Dalam era digital, keamanan siber telah muncul sebagai domain pertahanan yang kritis. Seperti yang diargumentasikan oleh Kello (2017), ancaman siber memiliki potensi untuk mengganggu infrastruktur kritis, merusak sistem keuangan, dan bahkan mempengaruhi proses demokrasi. Oleh karena itu, banyak negara telah mengembangkan strategi keamanan siber nasional sebagai bagian integral dari kebijakan pertahanan mereka (Klimburg, 2017).

Dalam kajian pertahanan kontemporer, konsep ketahanan masyarakat (social resilience) telah menjadi fokus utama selain komponen pertahanan non-militer lainnya. Ketahanan masyarakat merujuk pada kemampuan suatu bangsa atau komunitas untuk mempertahankan fungsi sosial dan ekonomi dalam menghadapi guncangan dan tekanan, baik yang berasal dari bencana alam, konflik, maupun krisis lainnya (Chandler, 2014). Konsep ini telah menjadi paradigma dominan dalam tata kelola risiko dan keamanan di banyak negara maju.

Sebagai contoh, Uni Eropa telah mengadopsi konsep "resilience" sebagai salah satu prinsip utama dalam Strategi Global untuk Kebijakan Luar Negeri dan Keamanan tahun 2016 (European Union, 2016). Dalam dokumen tersebut, resiliensi didefinisikan sebagai "kemampuan negara dan masyarakat untuk beradaptasi, bertransformasi, dan pulih secara cepat ketika menghadapi tekanan dan guncangan". Konsep ini juga menjadi fokus utama dalam strategi keamanan nasional beberapa negara, seperti Inggris (UK Government, 2015) dan Kanada (Government of Canada, 2017).

Di sisi lain, penelitian akademis menunjukkan bahwa konsep ketahanan masyarakat telah menjadi paradigma dominan dalam wacana keamanan dan manajemen risiko global (Chandler & Coaffee, 2017; Joseph, 2013). Para ahli berpendapat bahwa pendekatan ini memungkinkan pemerintah dan masyarakat untuk lebih proaktif dan adaptif dalam menghadapi ancaman dan tantangan yang semakin kompleks di era globalisasi.

Studi ini bertujuan untuk menganalisis dan membandingkan kebijakan pertahanan non-militer dari berbagai negara, termasuk Amerika Serikat, Cina, Rusia, Uni Eropa, Singapura, dan Australia. Tujuan utamanya adalah untuk: Mengidentifikasi tren global dalam pengembangan dan implementasi kebijakan pertahanan non-militer,

membandingkan pendekatan yang diambil oleh negara-negara berbeda dalam menghadapi tantangan keamanan non-tradisional, menganalisis efektivitas berbagai strategi pertahanan non-militer dalam konteks ancaman kontemporer, mengidentifikasi praktik terbaik dan inovasi dalam kebijakan pertahanan non-militer, dan merumuskan rekomendasi untuk pengembangan kebijakan pertahanan non-militer yang efektif dan adaptif.

METODE PENELITIAN

Penelitian ini mengadopsi pendekatan analisis komparatif kualitatif, mengintegrasikan tinjauan literatur komprehensif dengan analisis dokumen kebijakan resmi dan laporan pemerintah. Metodologi ini memungkinkan pemahaman mendalam tentang konteks, motivasi, dan implementasi kebijakan pertahanan non-militer di berbagai negara (George & Bennett, 2005).

Sumber data utama meliputi dokumen strategi keamanan nasional, white paper pertahanan, laporan kebijakan, dan publikasi akademik peer-reviewed. Analisis dilakukan dengan fokus pada empat pilar utama pertahanan non-militer: diplomasi, ketahanan ekonomi, keamanan siber, dan ketahanan masyarakat.

Pendekatan komparatif ini memungkinkan identifikasi pola, persamaan, dan perbedaan dalam kebijakan pertahanan non-militer antar negara, serta memberikan wawasan tentang faktor-faktor kontekstual yang mempengaruhi pengembangan kebijakan tersebut (Yin, 2018).

HASIL DAN PEMBAHASAN

A. Tren Global dalam Kebijakan Pertahanan Non-Militer

Analisis komparatif kebijakan pertahanan non-militer dari berbagai negara mengungkapkan beberapa tren global yang signifikan.

1. Integrasi Multidimensi

Temuan dari studi ini menunjukkan bahwa negara-negara semakin memprioritaskan pendekatan holistik dalam pertahanan, dengan penekanan khusus pada keamanan siber dan ketahanan ekonomi. Dua contoh yang menunjukkan persamaan ini adalah Amerika Serikat dan Cina.

Strategi Keamanan Nasional Amerika Serikat 2017 menekankan pentingnya mengintegrasikan berbagai instrumen kekuatan nasional, termasuk diplomasi, informasi, militer, ekonomi, keuangan, intelijen, dan penegakan hukum (White House, 2017). Dokumen ini menegaskan bahwa "kekuatan Amerika terletak pada gabungan instrumen nasionalnya" dan bahwa "keberhasilan akan bergantung pada kemampuan kami untuk mengintegrasikan instrumen ini secara efektif" (White House, 2017, p. 27).

Serupa dengan AS, Buku Putih Pertahanan Cina 2019 juga menekankan konsep "keamanan komprehensif" (comprehensive security) yang mencakup aspek politik, ekonomi, militer, budaya, dan sosial (State Council Information Office of China, 2019). Dokumen ini menyatakan bahwa Cina akan "menerapkan konsep keamanan komprehensif" dan "menguatkan sinkronisasi antara pembangunan ekonomi dan keamanan nasional" (State Council Information Office of China, 2019, p. 8).

Kedua negara ini memperlihatkan kesamaan dalam menekankan perlunya integrasi berbagai dimensi untuk memperkuat pertahanan nasional mereka. Baik AS maupun Cina menyadari bahwa ancaman keamanan kontemporer tidak lagi terbatas pada aspek militer saja, melainkan juga mencakup faktor-faktor non-militer

seperti keamanan siber, ketahanan ekonomi, dan stabilitas sosial-politik. Oleh karena itu, mereka berusaha mengadopsi pendekatan yang lebih holistik dan sinergis dalam merumuskan kebijakan pertahanan.

Dengan memadukan instrumen-instrumen kekuatan nasional secara efektif, AS dan Cina berharap dapat meningkatkan daya tahan dan kemampuan mereka dalam menghadapi berbagai ancaman kompleks di era globalisasi saat ini. Pendekatan ini mencerminkan pemahaman bahwa pertahanan nasional harus dipandang sebagai suatu sistem terintegrasi, bukan hanya sebagai kapabilitas militer semata.

Pendekatan multidimensi ini mencerminkan pemahaman yang berkembang bahwa ancaman keamanan kontemporer saling terkait dan memerlukan respons yang terkoordinasi. Seperti yang diargumentasikan oleh Cavelty dan Mauer (2020), kompleksitas ancaman modern membutuhkan "orkestrasi berbagai instrumen kebijakan" untuk pertahanan yang efektif.

2. Penekanan pada Ketahanan

Konsep ketahanan telah menjadi komponen inti dalam kebijakan pertahanan non-militer di banyak negara. Australia, misalnya, telah mengembangkan Strategi Ketahanan Nasional yang komprehensif, yang bertujuan untuk meningkatkan kemampuan negara untuk mengantisipasi, mencegah, merespons, dan pulih dari gangguan (Australian Government, 2020). Uni Eropa juga telah mengadopsi pendekatan serupa melalui "EU Approach to Resilience" yang menekankan pentingnya ketahanan dalam menghadapi berbagai ancaman, dari bencana alam hingga krisis ekonomi (European Commission, 2017).

Chandler (2014) berpendapat bahwa fokus pada ketahanan mencerminkan pergeseran dari paradigma keamanan tradisional yang berfokus pada pencegahan ancaman, menuju pendekatan yang lebih adaptif dan fleksibel. Pendekatan ini mengakui bahwa dalam dunia yang semakin tidak pasti, kemampuan untuk beradaptasi dan pulih dari guncangan sama pentingnya dengan mencegah ancaman.

3. Prioritas Keamanan Siber

Keamanan siber telah muncul sebagai domain prioritas dalam kebijakan pertahanan non-militer di semua negara yang dianalisis. Rusia, misalnya, telah mengembangkan Doktrin Keamanan Informasi yang komprehensif, yang menekankan pentingnya melindungi infrastruktur informasi kritis dan memerangi ancaman informasi (Ministry of Foreign Affairs of the Russian Federation, 2016). Singapura, dengan Strategi Keamanan Siber Nasionalnya, telah mengambil pendekatan proaktif dalam membangun ekosistem siber yang tangguh dan mengembangkan tenaga kerja keamanan siber yang kuat (Cyber Security Agency of Singapore, 2016).

Kello (2017) menyoroti bahwa keamanan siber telah menjadi "domain kelima" peperangan, sejajar dengan darat, laut, udara, dan ruang angkasa. Prioritas yang diberikan pada keamanan siber mencerminkan pengakuan akan potensi gangguan yang dapat ditimbulkan oleh serangan siber terhadap infrastruktur kritis, sistem ekonomi, dan proses demokratis.

B. Praktik Terbaik dan Inovasi

Analisis komparatif mengungkapkan beberapa praktik terbaik dan inovasi dalam kebijakan pertahanan non-militer:

1. Kemitraan Publik-Swasta

Banyak negara telah mengembangkan kemitraan publik-swasta yang kuat sebagai bagian dari strategi pertahanan non-militer mereka. Kemitraan ini memainkan peran

penting, terutama dalam domain keamanan siber, di mana sebagian besar infrastruktur kritis dimiliki dan dioperasikan oleh sektor swasta (Dunn Cavelty, 2013).

Sebagai contoh, Amerika Serikat telah membentuk National Cyber-Forensics and Training Alliance, sebuah kemitraan non-profit antara sektor publik, swasta, dan akademisi. Aliansi ini bertujuan untuk berbagi informasi intelijen dan memerangi ancaman siber yang semakin meningkat (FBI, 2021). Melalui kemitraan ini, pemerintah dapat memanfaatkan keahlian dan sumber daya sektor swasta, sementara sektor swasta mendapat akses ke informasi intelijen dan pelatihan yang diperlukan untuk meningkatkan pertahanan siber mereka.

Singapura juga telah meluncurkan inisiatif "SG Cyber Safe Partnership Programme" untuk melibatkan sektor swasta dalam meningkatkan keamanan siber nasional (Cyber Security Agency of Singapore, 2021). Program ini mendorong pertukaran informasi, koordinasi respons, dan pengembangan solusi inovatif antara pemerintah dan perusahaan swasta. Dengan memberdayakan sektor swasta, Singapura berhasil membangun ketahanan siber yang komprehensif dan responsif terhadap ancaman yang terus berevolusi.

Dunn Cavelty (2013) berpendapat bahwa kemitraan publik-swasta sangat penting dalam pertahanan non-militer karena memungkinkan pertukaran informasi yang lebih baik, koordinasi respons terhadap ancaman, dan pengembangan solusi inovatif. Selain itu, keterlibatan sektor swasta dapat meningkatkan efisiensi, fleksibilitas, dan daya tanggap terhadap tantangan keamanan yang cepat berubah. Kemitraan ini juga membantu mengatasi kesenjangan keahlian dan sumber daya antara sektor publik dan swasta.

Namun, membangun dan memelihara kemitraan publik-swasta yang efektif tidak selalu mudah. Tantangan yang sering dihadapi termasuk perbedaan budaya organisasi, masalah tata kelola, dan kekhawatiran tentang kerahasiaan informasi serta kepemilikan intelektual. Oleh karena itu, kerangka hukum dan tata kelola yang jelas sangat diperlukan untuk memastikan kemitraan tersebut berjalan lancar dan membawa manfaat bagi semua pihak yang terlibat.

2. Diplomasi Siber

Beberapa negara telah mengembang-kan konsep "diplomasi siber" sebagai bagian dari strategi pertahanan non-militer mereka. Australia, misalnya, telah menunjuk Duta Besar Urusan Siber untuk memimpin upaya diplomatik di bidang keamanan siber (Department of Foreign Affairs and Trade, Australia, 2021). Uni Eropa juga telah mengembangkan "EU Cyber Diplomacy Toolbox" yang menyediakan kerangka kerja untuk respons diplomatik terhadap aktivitas siber berbahaya (Council of the European Union, 2017).

Dalam lanskap keamanan global yang semakin kompleks, diplomasi siber telah menjadi semakin penting sebagai alat bagi negara-negara untuk mengelola konflik, membangun kepercayaan, dan menegakkan norma-norma perilaku yang bertanggung jawab di dunia maya (Barrinha & Renard, 2017). Namun, potensi konflik siber memiliki dinamika yang unik dan dapat menimbulkan ancaman serius terhadap keamanan nasional.

Konflik siber dapat terjadi dalam berbagai bentuk, mulai dari infiltrasi jaringan, sabotase infrastruktur digital, hingga operasi informasi yang bertujuan

untuk mempengaruhi opini publik (Rid, 2013). Serangan siber terhadap sistem vital, seperti jaringan listrik, sistem keuangan, atau layanan publik, dapat menimbulkan dampak yang signifikan pada ekonomi dan stabilitas sosial suatu negara (Sanger, 2018). Selain itu, ancaman siber dapat melintasi batas-batas geografis dan sulit untuk diatribusikan dengan pasti, membuatnya sangat menantang untuk ditangani melalui mekanisme pertahanan tradisional (Valeriano & Maness, 2015).

Lebih lanjut, operasi informasi yang dilakukan oleh aktor negara dapat memicu konflik dan ketegangan geopolitik. Penyebaran informasi yang menyesatkan, kampanye disinformasi, dan manipulasi media sosial dapat mengikis kepercayaan publik, memicu polarisasi, dan mengancam integritas proses demokrasi (Rid, 2020). Dalam konteks ini, diplomasi siber menjadi alat penting bagi negara-negara untuk menetapkan aturan main, membangun kerja sama internasional, dan mencegah eskalasi konflik di ranah siber.

Namun, upaya diplomasi siber itu sendiri juga menghadapi tantangan, karena kurangnya kerangka hukum dan normatif yang jelas, serta masalah atribusi serangan siber (Klimburg, 2017). Selain itu, kompetisi geopolitik dan rivalitas di antara negara-negara besar dapat menghambat kemajuan dalam pengembangan rezim tata kelola siber global yang efektif (Nye, 2017). Oleh karena itu, memahami dinamika konflik siber dan mendorong diplomasi siber yang efektif menjadi isu sentral dalam agenda pertahanan non-militer kontemporer.

3. Penggunaan Kecerdasan Buatan

Beberapa negara telah mulai mengintegrasikan teknologi kecerdasan buatan (AI) ke dalam strategi pertahanan non-militer mereka. China, misalnya, telah mengembangkan rencana untuk menjadi pemimpin global dalam AI, termasuk aplikasinya untuk keamanan nasional (State Council of China, 2017). Amerika Serikat juga telah mengakui pentingnya AI dalam pertahanan nasional, dengan Department of Defense merilis strategi AI yang komprehensif (U.S. Department of Defense, 2019).

Horowitz et al. (2018) menyoroti potensi AI untuk meningkatkan kemampuan pertahanan non-militer, termasuk dalam deteksi ancaman, analisis intelijen, dan pengambilan keputusan strategis. Namun, mereka juga memperingatkan tentang risiko yang terkait dengan AI, termasuk masalah etika dan potensi ketidakstabilan strategis. Meskipun ada kemajuan signifikan dalam pengembangan kebijakan pertahanan non-militer, beberapa tantangan dan keterbatasan tetap ada.

C. Koordinasi Antar Lembaga

Salah satu tantangan utama dalam implementasi kebijakan pertahanan non-militer adalah koordinasi yang efektif antar berbagai lembaga pemerintah. Di Amerika Serikat, misalnya, Government Accountability Office (2018) telah mengidentifikasi tumpang tindih dan duplikasi dalam upaya keamanan siber federal sebagai area yang membutuhkan perbaikan. Demikian pula, di Uni Eropa, koordinasi antara negara anggota dalam merespons ancaman hibrida tetap menjadi tantangan (European Court of Auditors, 2019).

Christensen dan Petersen (2017) berpendapat bahwa kompleksitas ancaman modern membutuhkan pendekatan "whole-of-government" yang lebih efektif, yang dapat sulit dicapai karena struktur birokrasi yang ada dan perbedaan budaya organisasi.

1. Adaptasi Terhadap Teknologi yang Berkembang Pesat

Kecepatan perkembangan teknologi menciptakan tantangan bagi pembuat kebijakan dalam mengembangkan dan mengimplementasikan strategi pertahanan non-militer yang efektif. Klimburg (2017) menyoroti bahwa siklus pengembangan kebijakan sering kali lebih lambat daripada evolusi ancaman teknologi, menciptakan "kesenjangan keamanan" yang dapat dieksploitasi oleh aktor berbahaya.

Tantangan ini terlihat jelas dalam domain keamanan siber, di mana teknik serangan baru terus bermunculan. Segal (2016) berpendapat bahwa negara-negara perlu mengembangkan mekanisme yang lebih fleksibel dan adaptif untuk merespons ancaman yang berkembang cepat ini.

2. Keseimbangan Keamanan dan Kebebasan Sipil

Implementasi kebijakan pertahanan non-militer, terutama yang berkaitan dengan pengawasan dan pengumpulan intelijen, sering kali menimbulkan ketegangan dengan kebebasan sipil dan privasi. Kasus Edward Snowden yang mengungkap program pengawasan NSA Amerika Serikat telah memicu debat global tentang batas-batas pengawasan pemerintah (Greenwald, 2014).

Deibert (2015) berpendapat bahwa negara-negara demokratis menghadapi tantangan khusus dalam menyeimbangkan kebutuhan keamanan dengan penghormatan terhadap hak-hak individu. Ia menyoroti pentingnya pengawasan demokratis dan transparansi dalam pengembangan dan implementasi kebijakan pertahanan non-militer. Deibert mencontohkan kasus Kanada, di mana upaya meningkatkan keamanan siber melalui pemantauan internet telah memicu protes dari kelompok hak asasi manusia yang mengklaim adanya pelanggaran privasi.

Scheppele (2006) juga mengkritik penggunaan argumen 'keamanan nasional' untuk membatasi kebebasan sipil, khususnya di era setelah 11 September 2001. Ia menyatakan bahwa keseimbangan yang tepat antara keamanan dan kebebasan sipil harus didasarkan pada prinsip-prinsip demokrasi dan hukum internasional. Scheppele berpendapat bahwa tanpa pengawasan dan pembatasan yang jelas, kebijakan pertahanan non-militer yang berlebihan dapat mengarah pada erosi hak-hak individu dan pengawasan yang berlebihan oleh negara.

Dalam konteks Uni Eropa, Bigo et al. (2014) menganalisis dilema keamanan-kebebasan dalam kebijakan keamanan internal. Mereka menemukan bahwa program pengawasan dan pertukaran data intelijen antara negara-negara anggota sering kali gagal mempertimbangkan implikasi terhadap privasi dan hak asasi manusia. Bigo et al. menyarankan perlunya reformasi kelembagaan yang memperkuat pengawasan demokratis dan akuntabilitas atas kegiatan intelijen.

Secara kritis, isu keseimbangan antara keamanan dan kebebasan sipil dalam kebijakan pertahanan non-militer mencerminkan tantangan fundamental dalam mempertahankan nilai-nilai demokratis di tengah ancaman keamanan yang terus berkembang. Meskipun pengawasan dan pengumpulan intelijen dapat meningkatkan keamanan nasional, pelaksanaannya harus tunduk pada mekanisme pengawasan yang ketat dan transparan untuk mencegah penyalahgunaan kekuasaan oleh negara. Negara-negara demokratis perlu secara hati-hati menyeimbangkan prioritas keamanan dengan perlindungan hak-hak

fundamental warga negaranya. Ketidakseimbangan yang berlebihan ke salah ssatu sisi dapat mengikis legitimasi pemerintah dan menimbulkan ketegangan sosial yang berkepanjangan.

D. Implikasi untuk Masa Depan

Berdasarkan analisis tren, praktik terbaik, dan tantangan dalam kebijakan pertahanan non-militer, beberapa implikasi untuk masa depan dapat diidentifikasi.

1. Peningkatan Fokus pada Ketahanan Sosial

Mengingat kompleksitas dan ketidakpastian ancaman modern, kemungkinan akan ada peningkatan fokus pada membangun ketahanan sosial sebagai komponen kunci pertahanan non-militer. Ini mungkin melibatkan investasi yang lebih besar dalam pendidikan publik, pelatihan kesiapsiagaan krisis, dan pengembangan jaringan sosial yang kuat.

Seperti yang diargumentasikan oleh Fjäder (2014), ketahanan sosial dapat menjadi "pertahanan terdepan" melawan berbagai ancaman, dari bencana alam hingga kampanye disinformasi. Negara-negara mungkin akan semakin mengadopsi pendekatan "whole-of-society" dalam pertahanan non-militer mereka.

2. Diplomasi Multilateral yang Lebih Kuat

Mengingat sifat transnasional dari banyak ancaman non-tradisional, kemungkinan akan ada dorongan yang lebih besar untuk kerja sama dan koordinasi internasional dalam pertahanan non-militer. Ini mungkin melibatkan pengembangan norma-norma dan standar internasional yang lebih kuat, terutama di bidang seperti keamanan siber dan penggunaan teknologi baru.

Nye (2020) berpendapat bahwa dalam era informasi global, "soft power" dan kemampuan untuk membentuk norma-norma internasional akan menjadi semakin penting dalam pertahanan nasional.

3. Integrasi Teknologi Canggih

Teknologi seperti kecerdasan buatan, blockchain, dan komputasi kuantum kemungkinan akan memainkan peran yang semakin penting dalam strategi pertahanan non-militer di masa depan. Negara-negara mungkin akan berinvestasi lebih banyak dalam pengembangan dan integrasi teknologi ini ke dalam sistem pertahanan mereka.

Namun, seperti yang diperingatkan oleh Brundage et al. (2018), penggunaan teknologi canggih dalam pertahanan juga membawa risiko baru, termasuk potensi perlombaan senjata teknologi dan masalah etika yang kompleks. Pembuat kebijakan perlu mengembangkan kerangka kerja yang kuat untuk mengelola risiko-risiko ini.

KESIMPULAN

Studi ini mengungkapkan bahwa negara-negara semakin mengadopsi pendekatan holistik dalam pertahanan non-militer, dengan integrasi berbagai dimensi keamanan termasuk diplomasi, ekonomi, keamanan siber, dan ketahanan sosial. Konsep ketahanan telah menjadi komponen inti, di mana negara-negara berinvestasi untuk meningkatkan kemampuan mengantisipasi, mencegah, merespons, dan pulih dari gangguan. Keamanan siber secara khusus telah menjadi prioritas utama, ditandai dengan pengembangan kemitraan publik-swasta dan konsep "diplomasi siber". Selain itu, negara-negara juga mulai mengintegrasikan teknologi canggih seperti kecerdasan buatan ke dalam strategi mereka. Namun, koordinasi yang efektif antarlembaga pemerintah, adaptasi terhadap perubahan teknologi yang cepat, serta menyeimbangkan keamanan dan kebebasan sipil tetap menjadi tantangan utama yang harus dihadapi. Ke depan,

rekomendasi kunci mencakup pengembangan pendekatan whole-of-government, penguatan investasi dalam ketahanan sosial dan kemitraan internasional, kerangka kebijakan yang fleksibel dan seimbang, serta peningkatan literasi digital dan kesadaran keamanan masyarakat.

DAFTAR PUSTAKA

Australian Government. (2020). A strategy for Australia's national resilience. Department of Home Affairs.

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. Global Affairs, 3(4-5), 353-364.

Barrinha, A., & Renard, T. (2017). Cyberdiplomacy: the making of an international society in the digital age. Global Affairs, 3(4-5), 353-364.

Brooks, S. G., & Wohlforth, W. C. (2016). The rise and fall of the great powers in the twenty-first century: China's rise and the fate of America's global position. International Security, 40(3), 7-53.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228.

Cavelty, M. D., & Mauer, V. (2020). Routledge handbook of security studies. Routledge.

Chandler, D. (2014). Resilience: The governance of complexity. Routledge.

Chandler, D., & Coaffee, J. (Eds.). (2017). The Routledge Handbook of International Resilience. Routledge.

Christensen, K. K., & Petersen, K. L. (2017). Public–private partnerships on cyber security: a practice of loyalty. International Affairs, 93(6), 1435-1452.

Council of the European Union. (2017). Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").

Cyber Security Agency of Singapore. (2016). Singapore's Cybersecurity Strategy.

Cyber Security Agency of Singapore. (2021). SG Cyber Safe Partnership Programme. Diakses dari https://www.csa.gov.sg/programmes/sg-cyber-safe-partnership-programme

Deibert, R. J. (2015). The geopolitics of cyberspace after Snowden. Current History, 114(768), 9-15.

Department of Foreign Affairs and Trade, Australia. (2021). Australia's International Cyber Engagement Strategy.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. International Studies Review, 15(1), 105-122. doi:10.1111/misr.12023

European Commission. (2017). A Strategic Approach to Resilience in the EU's External Action.

European Union. (2016). Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign and Security Policy.

FBI. (2021). National Cyber-Forensics and Training Alliance. Diakses dari https://www.fbi.gov/investigate/cyber/national-cyber-forensics-and-training-alliance

George, A. L., & Bennett, A. (2005). Case studies and theory development in the social sciences. MIT Press.

Government of Canada. (2017). 2017 Public Report on the Terrorist Threat to Canada.

Joseph, J. (2013). Resilience as embedded neoliberalism: a governmentality approach. Resilience, 1(1), 38-52.

Kello, L. (2017). The virtual weapon and international order. Yale University Press.

Klimburg, A. (2017). The darkening web: The war for cyberspace. Penguin.

Nye, J. S. (2011). The future of power. Public Affairs.

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44-71.

Rid, T. (2013). Cyber war will not take place. Journal of strategic studies, 35(1), 5-32.

Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.

Sanger, D. E. (2018). The perfect weapon: War, sabotage, and fear in the cyber age. Broadway Books.

State Council Information Office of China. (2019). China's National Defense in the New Era. http://www.xinhuanet.com/english/2019-07/24/c_138253389.htm

UK Government. (2015). National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom.

Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press.

White House. (2017). National Security Strategy of the United States of America. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Yin, R. K. (2018). Case study research and applications: Design and methods. Sage publications.