Jurnal Praksis dan Dedikasi (JPDS)
April, 2025, Vol. 8, No. 1 hal. 118-132
http://dx.doi.org/10.17977/um022v8i12025p118-132

Menghadapi ancaman siber di era society 5.0: Inovasi strategi diplomasi pertahanan untuk stabilitas sosial

Addressing cyber threats in the society 5.0 era: Strategic innovations in defense diplomacy for social stability

Alice Agatha Delfreeta Aritonang

*Corresponding author, Email: alice.agatha13@gmail.com

Universitas Pertahanan, Kawasan IPSC Sentul, Sukahati, Kec. Citeureup, Kabupaten Bogor, Jawa Barat, 16810, Indonesia

Paper received: 25-07-2024; revised: 03-12-2024; accepted: 28-02-2025; published: 30-04-2025

How to cite (APA Style): Aritonang, A. A. D. (2025). Menghadapi ancaman siber di era society 5.0: Inovasi strategi diplomasi pertahanan untuk stabilitas sosial. *Jurnal Praksis dan Dedikasi Sosial (JPDS), 8*(1), 118-132. DOI: 10.17977/um022v8i12025p118-132

Abstract

The Society 5.0 era introduces the integration of advanced technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), big data, and robotics into the social, political, and economic spheres of global society. Japan, as the pioneer of Society 5.0, formulated this concept as a response to various social challenges, including those related to security and defense diplomacy. This article examines the implications of Society 5.0 for defense diplomacy, particularly in strategies for cyber and non-traditional security, aimed at safeguarding national security and social stability amid technological change. Using a literature review approach and secondary data analysis, this study identifies three key strategies: national security, technological enhancement, and international collaboration. The analysis reveals that defense diplomacy now involves collaborative approaches and digital strategy to respond to modern threats. These findings highlight the importance of international cooperation and increased technological literacy at the community level to support social security in the Society 5.0 era.

Keywords: society 5.0; defense diplomacy; cybersecurity; international collaboration

Abstrak

Era Society 5.0 memperkenalkan integrasi teknologi tinggi seperti kecerdasan buatan (AI), Internet of Things (IoT), big data, dan robotika dalam kehidupan sosial, politik, dan ekonomi masyarakat global. Jepang sebagai pelopor Society 5.0 merumuskan konsep ini sebagai jawaban atas berbagai tantangan sosial, termasuk di bidang keamanan dan diplomasi pertahanan. Artikel ini mengkaji implikasi Society 5.0 dalam diplomasi pertahanan, khususnya pada strategi keamanan siber dan non-tradisional, yang bertujuan untuk melindungi keamanan nasional dan stabilitas sosial di tengah perubahan teknologi. Dengan menggunakan pendekatan literature review dan analisis data sekunder, penelitian ini menemukan tiga strategi utama: keamanan nasional, penguatan teknologi, dan kolaborasi internasional. Hasil analisis menunjukkan bahwa diplomasi pertahanan kini melibatkan pendekatan kolaboratif dan strategi digital untuk merespons ancaman modern. Temuan ini menegaskan pentingnya kolaborasi internasional dan peningkatan literasi teknologi pada tingkat komunitas dalam mendukung keamanan sosial di era Society 5.0.

Kata kunci: society 5.0; diplomasi pertahanan; keamanan siber; kolaborasi internasional

PENDAHULUAN

Society 5.0 adalah konsep yang diperkenalkan oleh Jepang sebagai respon terhadap era industri 4.0. *Society* 5.0 dirancang untuk menciptakan masyarakat yang sepenuhnya terintegrasi dengan teknologi canggih seperti kecerdasan buatan (AI), *Internet of Things* (IoT), big data, dan robotika, yang dimanfaatkan untuk meningkatkan kesejahteraan sosial, ekonomi, dan keamanan (Deguchi et al., 2020). Tidak seperti industri 4.0 yang berfokus pada efisiensi dan produktivitas, Society 5.0 berfokus pada pendekatan human-centered, di mana teknologi menjadi sarana untuk mengatasi berbagai permasalahan sosial, seperti ketimpangan ekonomi, perubahan demografi, dan tantangan lingkungan (Fukuyama, 2018). Di tengah percepatan digitalisasi, *Society* 5.0 membuka peluang besar untuk mengintegrasikan teknologi dalam berbagai sektor, termasuk pertahanan nasional, guna mendukung keamanan dan stabilitas negara.

Dalam konteks pertahanan nasional, *Society* 5.0 memperkenalkan perubahan signifikan dalam cara negara mengelola dan merespons ancaman keamanan. Dengan adanya *Society* 5.0, ancaman tradisional seperti invasi militer mulai bertransformasi menjadi ancaman non-tradisional yang mencakup serangan siber, spionase digital, dan sabotase melalui jaringan komputer. Ketergantungan pada teknologi digital juga meningkatkan potensi kerentanan yang dapat dimanfaatkan oleh aktor negara dan non-negara untuk melancarkan serangan. Oleh karena itu, pemerintah dan instansi terkait harus beradaptasi dan mengembangkan strategi pertahanan yang tidak hanya mampu menghadapi ancaman fisik tetapi juga ancaman digital yang kian kompleks dan lintas batas (Hoadley & Lucas, 2018).

Diplomasi pertahanan telah mengalami perubahan signifikan dengan adanya perkembangan teknologi digital. Menurut Hoadley dan Lucas (2018), pendekatan keamanan siber dalam hubungan internasional menjadi semakin penting, terutama dalam menghadapi ancaman yang bersifat non-tradisional seperti serangan siber dan spionase digital. Beberapa negara telah mengadaptasi teknologi kecerdasan buatan (AI) dan big data dalam pengelolaan risiko keamanan nasional (Schmidt & Cohen, 2019). Keamanan siber telah menjadi prioritas dalam kebijakan pertahanan modern. Negara-negara maju seperti Amerika Serikat dan Tiongkok telah mengembangkan strategi keamanan berbasis AI untuk mendeteksi dan merespons ancaman secara real-time (KPMG, 2021). Menurut Giannopoulos, Smith, dan Schleiss (2021), pemanfaatan IoT dalam keamanan siber memungkinkan pemantauan ancaman yang lebih efektif, sementara big data membantu dalam analisis tren serangan siber. Studi ini menyoroti bagaimana Indonesia dapat mengadaptasi strategi serupa dalam diplomasi pertahanannya.

Ancaman siber bersifat lintas batas dan membutuhkan kerja sama antarnegara untuk mitigasi yang efektif. Laporan National Cyber Security Centre (2022) menegaskan pentingnya pertukaran informasi dan standar keamanan bersama dalam diplomasi pertahanan global. ASEAN telah memperkenalkan ASEAN Cybersecurity Cooperation Strategy untuk memperkuat koordinasi keamanan siber di kawasan Asia Tenggara (OECD, 2022). Indonesia menghadapi ancaman siber yang semakin meningkat. Laporan BSSN (2022) mencatat lonjakan insiden siber sebesar 25% dibandingkan tahun sebelumnya, dengan sektor energi, komunikasi, dan keuangan sebagai target utama. Prakoso (2020) menyoroti bahwa strategi pertahanan siber Indonesia masih dalam tahap pengembangan dan memerlukan kebijakan yang lebih komprehensif untuk menghadapi ancaman yang semakin kompleks. Penelitian ini akan menyoroti langkah-langkah yang dapat diambil untuk memperkuat pertahanan siber Indonesia melalui diplomasi pertahanan di era Society 5.0.

Penelitian ini bertujuan untuk mengkaji tantangan dan peluang yang muncul dalam diplomasi pertahanan di era *Society* 5.0, serta merumuskan strategi yang tepat untuk menghadapi ancaman baru. Dengan menggunakan metode literature review, penelitian ini menelaah adopsi teknologi dalam pertahanan nasional, khususnya di Indonesia, dan mengeksplorasi bagaimana diplomasi pertahanan dapat beradaptasi untuk menangani tantangan

keamanan siber yang semakin berkembang. Tujuan utama penelitian ini adalah untuk memahami bagaimana *Society* 5.0 mengubah pendekatan dalam diplomasi pertahanan, baik dari aspek kerjasama internasional maupun dalam peningkatan kapabilitas teknologi dalam negeri. Studi ini juga bertujuan untuk menyoroti peran teknologi digital dalam memperkuat sistem pertahanan, termasuk pemanfaatan AI, IoT, dan big data dalam deteksi dini ancaman, pengawasan perbatasan, serta perlindungan terhadap infrastruktur kritis. Dengan demikian, penelitian ini akan memberikan panduan bagi pembuat kebijakan mengenai bagaimana teknologi dapat digunakan untuk memperkuat strategi diplomasi pertahanan di tengah perkembangan ancaman siber dan digital yang semakin pesat.

Signifikansi studi ini terletak pada kontribusinya dalam memberikan pemahaman yang lebih mendalam tentang bagaimana *Society* 5.0 mempengaruhi pendekatan keamanan nasional dan pertahanan di Indonesia. Dalam era *Society* 5.0, diplomasi pertahanan tidak lagi hanya berfokus pada kekuatan militer konvensional tetapi juga memerlukan kemampuan dalam menghadapi ancaman digital. *Society* 5.0 menuntut negara-negara untuk mengintegrasikan strategi pertahanan fisik dan digital secara bersamaan guna memastikan keamanan nasional. Melalui integrasi teknologi seperti AI dan IoT dalam sistem pertahanan, negara dapat meningkatkan kemampuan deteksi dini, manajemen risiko, serta kesiapsiagaan dalam menghadapi ancaman non-tradisional yang terus berkembang.

Penelitian ini penting karena memberikan pandangan baru bagi pemerintah dan pemangku kepentingan tentang urgensi kolaborasi internasional dan inovasi teknologi dalam menjaga stabilitas keamanan nasional. Hasil dari studi ini diharapkan dapat mendorong kebijakan yang lebih adaptif dan progresif dalam diplomasi pertahanan di Indonesia, sehingga negara dapat menghadapi tantangan *Society* 5.0 dengan strategi yang efektif dan berkelanjutan. Dengan demikian, penelitian ini tidak hanya relevan dalam konteks diplomasi pertahanan tetapi juga dalam kebijakan keamanan nasional yang lebih luas.

Society 5.0 adalah konsep yang dicetuskan Jepang untuk mewujudkan masyarakat yang sepenuhnya terintegrasi dengan teknologi tinggi seperti AI, IoT, big data, dan robotika. *Society* 5.0 didesain untuk menyelesaikan berbagai permasalahan sosial dan menciptakan masyarakat yang lebih sejahtera dan inklusif melalui pemanfaatan teknologi canggih (Deguchi et al., 2020). Integrasi teknologi dalam kehidupan sehari-hari bertujuan untuk meningkatkan produktivitas, mempercepat inovasi, serta menciptakan solusi untuk masalah-masalah sosial, seperti ketimpangan ekonomi, perubahan demografi, dan tantangan lingkungan (Fukuyama, 2018). Konsep *Society* 5.0 tidak hanya terbatas pada aspek ekonomi, tetapi juga melibatkan sektor kesehatan, pendidikan, dan keamanan.

Implementasi *Society* 5.0 berdampak luas pada masyarakat, terutama dalam hal cara teknologi digunakan untuk menciptakan nilai tambah di berbagai sektor. Dalam bidang pertahanan, *Society* 5.0 mengarah pada peningkatan efektivitas dan efisiensi melalui otomatisasi, analisis data yang akurat, dan pengawasan yang canggih. Teknologi tinggi ini tidak hanya digunakan untuk keperluan bisnis tetapi juga untuk meningkatkan keamanan dan stabilitas nasional. *Society* 5.0 mendorong penggunaan data dan analitik prediktif untuk mendeteksi dan mencegah potensi ancaman, baik dari aktor negara maupun non-negara, sehingga teknologi tidak hanya berperan sebagai alat ekonomi tetapi juga sebagai instrumen penting dalam diplomasi pertahanan.

Ancaman siber yang semakin kompleks menuntut negara-negara untuk memprioritaskan diplomasi pertahanan yang terfokus pada keamanan digital. Menurut Prakoso (2020), Indonesia menghadapi tantangan besar di Laut Cina Selatan, di mana ancaman siber dan ketegangan regional memerlukan strategi diplomatik yang kuat dan kerjasama keamanan untuk mempertahankan stabilitas dan menjaga posisi strategis Indonesia dalam percaturan global.

Dengan semakin luasnya adopsi teknologi digital, ancaman siber menjadi masalah serius di era *Society* 5.0. Ancaman siber memiliki sifat yang lintas batas dan dapat berdampak besar

pada stabilitas nasional dan internasional. Menurut Hoadley dan Lucas (2018), meningkatnya ketergantungan pada teknologi tinggi juga meningkatkan kerentanan terhadap ancaman siber, khususnya pada sektor-sektor kritis seperti energi, komunikasi, dan transportasi. Ancaman siber ini tidak hanya merugikan secara finansial, tetapi juga dapat mengancam keamanan nasional suatu negara, sehingga memerlukan perhatian khusus dalam strategi diplomasi pertahanan.

Laporan National Cyber Security Centre (2022) menyoroti pentingnya kerja sama internasional untuk menghadapi ancaman siber yang semakin kompleks. Negara-negara perlu berkolaborasi dalam membangun standar keamanan bersama, pertukaran informasi, serta koordinasi dalam menangani insiden siber. Diplomasi pertahanan memainkan peran penting dalam membangun kemitraan ini, yang tidak hanya membantu mengelola risiko keamanan siber tetapi juga membentuk kepercayaan antarnegara. Melalui diplomasi pertahanan yang kuat, negara-negara dapat meningkatkan pertahanan siber mereka dengan dukungan dari komunitas internasional, yang pada akhirnya membantu menjaga stabilitas global di era digital.

Di era *Society* 5.0, diplomasi pertahanan menghadapi tantangan baru dalam mengintegrasikan teknologi digital ke dalam strategi keamanan nasional. Pramono (2023) mengemukakan bahwa diplomasi pertahanan harus mampu merespons ancaman non-tradisional, termasuk ancaman siber yang seringkali melibatkan aktor non-negara seperti kelompok kriminal atau peretas independen. Diplomasi pertahanan di era digital harus fleksibel dan inovatif untuk menghadapi ancaman yang terus berubah, terutama ancaman yang terkait dengan keamanan siber.

Schmidt dan Cohen (2019) menyoroti pentingnya pendekatan yang kolaboratif dalam diplomasi pertahanan di era digital, di mana negara-negara dapat berbagi teknologi, informasi, dan strategi untuk menangani ancaman siber. Strategi ini mencakup pengembangan sistem keamanan yang lebih terintegrasi dan real-time, dengan bantuan teknologi seperti AI dan IoT untuk mendeteksi dan merespons ancaman secara lebih efektif. Dengan demikian, diplomasi pertahanan di era *Society 5.0* tidak hanya mencakup kekuatan militer konvensional, tetapi juga mencakup kemampuan dalam bidang keamanan siber untuk menjaga stabilitas nasional dan internasional.

Diplomasi pertahanan di era *Society 5.0* juga mengintegrasikan pendekatan "Total War" atau perang menyeluruh untuk mendukung kekuatan pertahanan. Dalam konteks Indonesia, Prakoso dan Taryanto (2022) menyoroti pentingnya kolaborasi antara sektor sipil dan militer, termasuk peran galangan kapal nasional, dalam memperkuat ketahanan maritim melalui strategi menyeluruh yang berbasis teknologi.

Indonesia telah mengambil berbagai inisiatif untuk meningkatkan keamanan siber dan mengintegrasikan *Society* 5.0 dalam kebijakan pertahanan nasional. Kementerian Komunikasi dan Informatika (Kominfo) pada 2022 meluncurkan berbagai program yang mendorong adopsi teknologi digital di sektor publik, termasuk dalam pengelolaan keamanan siber. Kominfo juga mendorong peningkatan literasi digital di kalangan masyarakat untuk memperkuat ketahanan siber dari level pengguna hingga pemerintah (Kominfo, 2022).

Badan Siber dan Sandi Negara (BSSN) memainkan peran kunci dalam meningkatkan kemampuan pertahanan siber Indonesia. Pada 2022, BSSN melaporkan peningkatan adopsi teknologi siber dalam diplomasi pertahanan, seperti penerapan sistem deteksi ancaman otomatis yang didukung oleh AI. BSSN juga berkolaborasi dengan berbagai negara dan organisasi internasional untuk memperkuat pertukaran informasi dan peningkatan kemampuan dalam menangani ancaman siber (BSSN, 2022). Inisiatif ini menunjukkan komitmen Indonesia dalam memperkuat pertahanan nasional melalui diplomasi siber dan pengintegrasian *Society* 5.0, yang mendukung keamanan nasional di era digital.

METODE

Pendekatan Studi

Literatur yang digunakan dalam penelitian ini dipilih berdasarkan kriteria inklusi dan eksklusi yang ketat untuk memastikan relevansi dan kredibilitas sumber. Kriteria inklusi meliputi publikasi dalam jurnal ilmiah bereputasi, buku akademik, serta laporan dari lembaga internasional seperti OECD, NATO CCDCOE, dan ITU. Selain itu, hanya studi yang diterbitkan dalam lima tahun terakhir yang digunakan untuk memastikan keterbaruan informasi, serta artikel yang secara khusus membahas diplomasi pertahanan, keamanan siber, dan integrasi teknologi dalam kebijakan keamanan nasional. Sementara itu, kriteria eksklusi mencakup publikasi yang tidak melalui proses peer-review atau berasal dari sumber yang tidak kredibel, artikel yang tidak relevan dengan fokus penelitian ini, seperti yang hanya membahas teknologi tanpa keterkaitan dengan kebijakan pertahanan, serta studi dengan metodologi yang tidak jelas atau tidak didukung oleh data yang memadai. Sumber-sumber yang memenuhi kriteria tersebut kemudian dianalisis menggunakan pendekatan deskriptif dan tematik untuk mengidentifikasi pola, tantangan, serta peluang yang relevan dengan diplomasi pertahanan di era *Society 5.0*. Dengan memasukkan perspektif dari penelitian sebelumnya, studi ini diharapkan dapat memberikan kontribusi signifikan terhadap pemahaman mengenai peran *Society 5.0* dalam diplomasi pertahanan dan keamanan siber di Indonesia.

Sumber Data dan Pengumpulan Informasi

Data dalam penelitian ini dikumpulkan dari berbagai sumber yang kredibel dan relevan. Sumber pertama berasal dari jurnal akademik, baik internasional maupun nasional, yang digunakan sebagai referensi utama untuk memahami bagaimana teknologi *Society* 5.0 memengaruhi diplomasi pertahanan. Beberapa artikel yang dikaji mencakup pembahasan mengenai ancaman siber, penerapan *Artificial Intelligence* (AI) dan *Internet of Things* (IoT) dalam bidang pertahanan, serta konsep diplomasi pertahanan di era digital.

Sumber kedua berasal dari laporan pemerintah. Data yang diperoleh dari instansi seperti Badan Pusat Statistik (BPS) dan Badan Siber dan Sandi Negara (BSSN) memberikan informasi penting mengenai tingkat adopsi teknologi serta gambaran umum mengenai ancaman siber di Indonesia. Laporan-laporan ini menjadi dasar dalam memahami implementasi *Society* 5.0 khususnya dalam sektor pertahanan dan keamanan nasional.

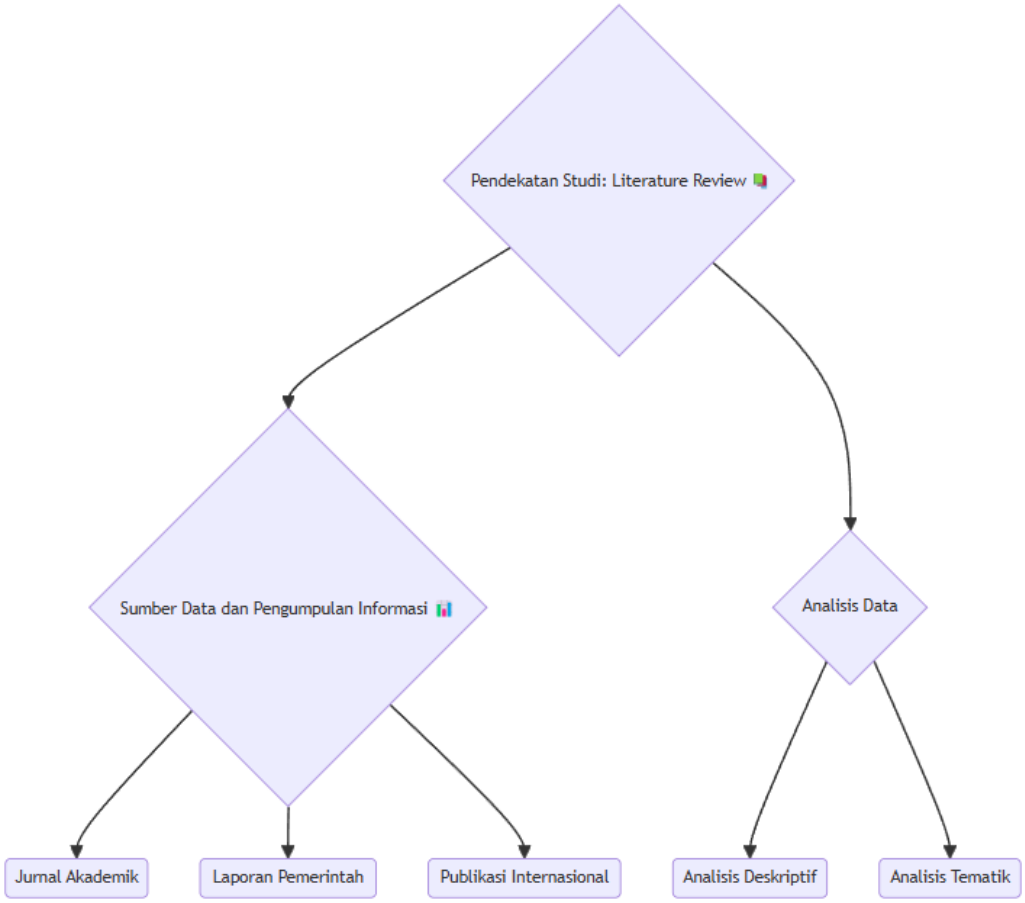
Selain itu, publikasi internasional juga dijadikan referensi untuk memperdalam analisis. Penelitian ini merujuk pada laporan dari lembaga-lembaga internasional seperti OECD dan *Global Cybersecurity Index*. Publikasi tersebut memberikan perspektif global terkait tren keamanan siber dan berbagai langkah strategis yang diterapkan oleh negara-negara lain. Informasi ini berguna sebagai bahan perbandingan dalam menganalisis kebijakan diplomasi pertahanan di Indonesia.

Analisis Data

Analisis data dilakukan dengan metode deskriptif dan tematik untuk menyusun temuan-temuan utama terkait diplomasi pertahanan di era *Society* 5.0. Analisis deskriptif digunakan untuk memaparkan data kuantitatif dan kualitatif yang diperoleh dari sumber-sumber sekunder, seperti statistik adopsi teknologi, tren ancaman siber, dan langkah-langkah kebijakan yang telah diambil oleh pemerintah. Pendekatan ini membantu dalam menggambarkan kondisi diplomasi pertahanan Indonesia dan mengidentifikasi faktor-faktor yang mempengaruhi implementasi *Society* 5.0.

Analisis tematik dilakukan untuk mengidentifikasi tema-tema utama dalam literatur terkait, seperti peran AI dalam diplomasi pertahanan, tantangan keamanan siber, serta peluang

kolaborasi internasional. Dengan mengidentifikasi pola dan tema yang muncul dalam berbagai literatur, penelitian ini dapat menyusun rekomendasi strategis yang relevan untuk menghadapi tantangan *Society* 5.0 dalam konteks diplomasi pertahanan. Pendekatan ini memungkinkan penelitian untuk menyajikan temuan yang sistematis dan berfokus pada elemen-elemen kunci yang diperlukan dalam membangun diplomasi pertahanan yang adaptif di era digital. Gambar 1 menunjukkan paradigma penelitian.



Gambar 1. Paradigma Penelitian

HASIL DAN PEMBAHASAN

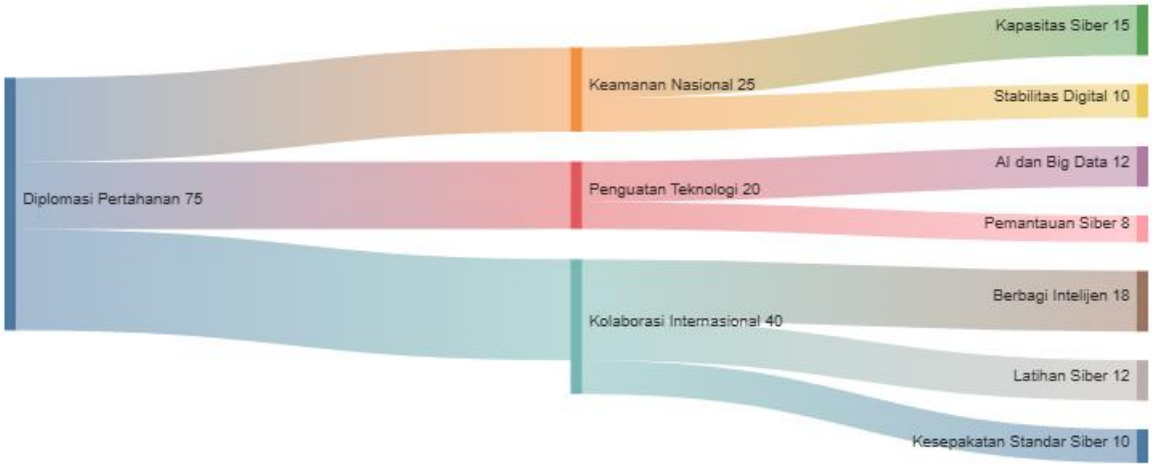
Studi ini menyoroti bahwa adaptasi diplomasi pertahanan terhadap *Society* 5.0 memerlukan strategi komprehensif yang mencakup inovasi teknologi serta kerja sama internasional. Berbeda dengan penelitian sebelumnya yang lebih menekankan pada aspek teknis keamanan siber, studi ini menawarkan perspektif holistik yang menghubungkan teknologi dengan kebijakan pertahanan (Schmidt & Cohen, 2019; Prakoso, 2020). Analisis ini menunjukkan bahwa negara-negara yang lebih maju telah mengembangkan kebijakan yang lebih proaktif, sementara Indonesia masih berada dalam tahap awal implementasi strategi berbasis teknologi.

Implikasi teoretis dari studi ini adalah bahwa diplomasi pertahanan dalam era *Society* 5.0 tidak lagi terbatas pada kekuatan militer konvensional, tetapi juga melibatkan integrasi strategi siber dalam kebijakan luar negeri. Secara praktis, penelitian ini menggarisbawahi perlunya peningkatan kapasitas sumber daya manusia di sektor pertahanan serta investasi dalam teknologi berbasis AI dan big data untuk deteksi dini ancaman.

Tren dan Penerapan *Society* 5.0 di Indonesia

Implementasi *Society* 5.0 di Indonesia semakin meningkat dalam beberapa tahun terakhir, dengan penggunaan AI, IoT, dan big data yang mulai terintegrasi di sektor publik dan swasta. Teknologi ini tidak hanya mendukung produktivitas ekonomi tetapi juga memainkan peran penting dalam mendukung keamanan dan stabilitas nasional. Di sektor publik, berbagai inisiatif telah dijalankan oleh pemerintah melalui lembaga-lembaga seperti Kementerian Komunikasi dan Informatika (Kominfo) dan Badan Pusat Statistik (BPS) untuk meningkatkan efisiensi layanan dengan pemanfaatan big data dan IoT dalam manajemen data dan analisis kebijakan (Kominfo, 2022; BPS, 2021). Misalnya, big data digunakan untuk membantu perencanaan kota pintar, manajemen lalu lintas, dan pengawasan publik secara *real-time*.

Di sektor swasta, penggunaan AI dan IoT juga meningkat, terutama dalam sektor finansial, manufaktur, dan agrikultur. Dalam sektor finansial, AI digunakan untuk meningkatkan keamanan transaksi, mengidentifikasi pola ancaman, serta mempersonalisasi layanan kepada konsumen. Sektor agrikultur memanfaatkan IoT untuk memonitor kondisi cuaca, kelembaban tanah, dan pertumbuhan tanaman, yang telah meningkatkan efisiensi dan hasil panen hingga 20% (Statista, 2022). Di industri manufaktur, AI dan IoT digunakan dalam otomatisasi produksi, pemantauan kondisi mesin secara *real-time*, dan prediksi perawatan, yang meningkatkan efisiensi operasional. Gambar 2 menunjukkan aliran diplomasi pertahanan dalam Era *Society* 5.0.



Gambar 2. Aliran Diplomasi Pertahanan dalam Era *Society* 5.0

Gambar 2 (*Diagram Sankey*) yang digunakan dalam penelitian ini menunjukkan bahwa alokasi terbesar dalam diplomasi pertahanan era *Society* 5.0 adalah pada kolaborasi internasional. Hal ini mencerminkan bahwa ancaman siber bersifat lintas negara dan memerlukan respons kolektif. Studi ini juga mengusulkan bahwa model kerja sama ASEAN dapat menjadi kerangka kerja utama dalam membangun keamanan siber regional yang lebih kuat.

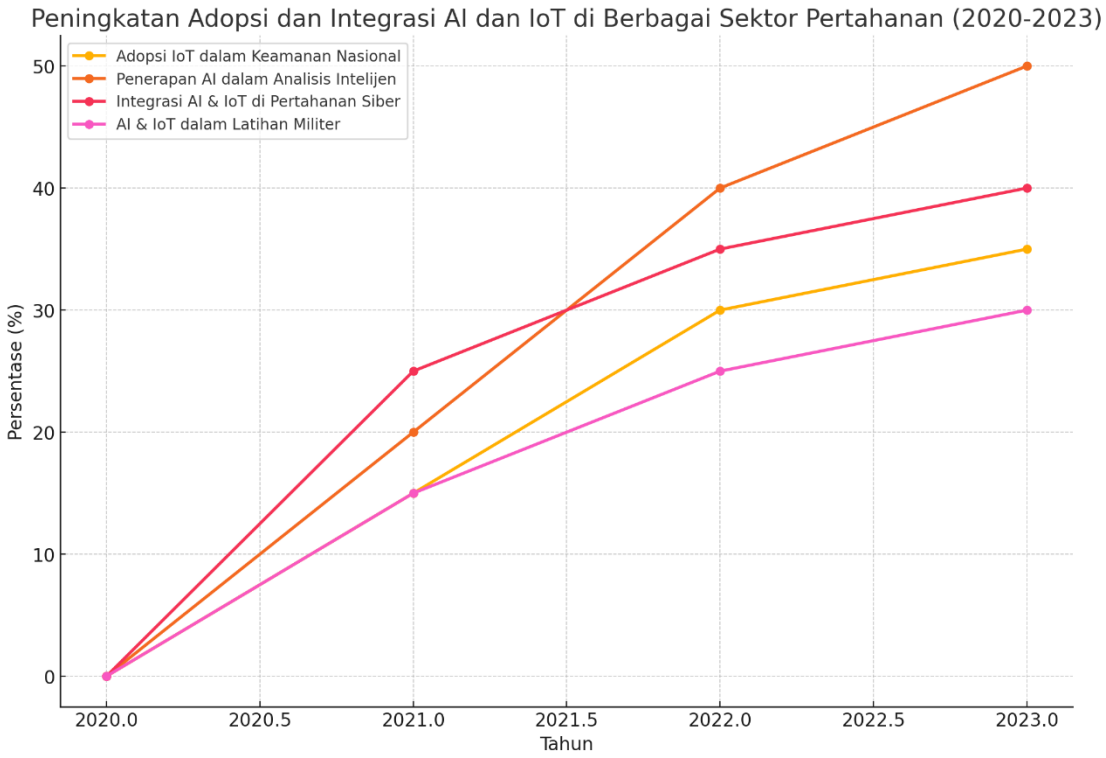
Dengan demikian, penelitian ini memberikan wawasan yang lebih luas tentang bagaimana *Society* 5.0 dapat diadopsi untuk memperkuat strategi diplomasi pertahanan, sekaligus memberikan panduan bagi pembuat kebijakan dalam merancang kebijakan pertahanan yang lebih adaptif dan berbasis teknologi.

Analisis mendalam terhadap setiap komponen menunjukkan bagaimana diplomasi pertahanan diarahkan untuk mendukung berbagai aspek strategis dalam menghadapi tantangan era digital. Salah satu aliran utama adalah dari diplomasi pertahanan ke keamanan nasional, yang mencakup 25% dari total fokus. Alokasi ini terdiri dari penguatan kapasitas siber sebesar 15% dan stabilitas digital sebesar 10%. Fokus ini menunjukkan bahwa pertahanan digital menjadi

prioritas utama dalam menjaga keamanan nasional, terutama dalam menghadapi ancaman siber yang semakin kompleks dan terstruktur.

Selanjutnya, diplomasi pertahanan juga mengalir ke arah penguatan teknologi, yang mencakup 20% dari keseluruhan strategi. Dalam aliran ini, pengembangan teknologi seperti *Artificial Intelligence* (AI) dan *Big Data* mendapat porsi sebesar 12%, sementara pemantauan siber mendapat alokasi sebesar 8%. Ini menegaskan bahwa teknologi bukan sekadar alat bantu, melainkan fondasi penting dalam membangun sistem pertahanan siber yang adaptif dan responsif terhadap berbagai jenis ancaman.

Komponen terbesar dari strategi ini adalah aliran diplomasi pertahanan ke kolaborasi internasional, dengan alokasi sebesar 30%. Besarnya porsi ini mencerminkan urgensi dan pentingnya kerja sama antarnegara dalam menghadapi ancaman global yang tidak mengenal batas wilayah. Kolaborasi ini mencakup berbagi intelijen (18%), pelaksanaan latihan siber bersama (12%), dan kesepakatan mengenai standar siber internasional (10%). Fokus ini memperlihatkan bahwa diplomasi pertahanan modern berperan penting tidak hanya dalam menjaga keamanan internal, tetapi juga dalam membangun sistem pertahanan kolektif yang melibatkan negara-negara mitra. Gambar 3 menunjukkan peningkatan adopsi dan integrasi AI serta IoT di berbagai sektor pertahanan di Indonesia Periode 2020-2023.



Gambar 3. Peningkatan Adopsi dan Integrasi AI serta IoT di berbagai Sektor Pertahanan di Indonesia Periode 2020-2023

Berikut adalah gambaran umum tentang pertumbuhan adopsi AI dan IoT dalam diplomasi pertahanan di Indonesia dari 2020 hingga 2023, dengan fokus pada sektor-sektor utama seperti keamanan nasional, pengelolaan data intelijen, dan peningkatan kapabilitas militer.

Adopsi IoT dalam Keamanan Nasional dan Pengawasan Perbatasan

Pada tahun 2020, penggunaan *Internet of Things* (IoT) dalam diplomasi pertahanan di Indonesia masih berada pada tahap awal. Implementasi teknologi ini difokuskan pada proyek-

proyek percontohan, terutama untuk pemantauan perbatasan dan pengawasan daerah rawan konflik. Sistem yang dikembangkan bertujuan untuk mendeteksi potensi ancaman di wilayah perbatasan serta menyediakan informasi secara waktu nyata bagi pengambil keputusan.

Memasuki tahun 2021, terjadi peningkatan sebesar 15% dalam penggunaan perangkat IoT di sektor keamanan nasional. Fokus utama pengembangan diarahkan pada pengawasan perbatasan di wilayah perairan dan udara. Teknologi berbasis IoT mulai diterapkan di sejumlah lokasi strategis guna mendeteksi aktivitas ilegal dan mendukung tugas penjagaan perbatasan secara lebih efektif (Kominfo, 2022).

Pada tahun 2022, implementasi IoT dalam pengawasan daerah perbatasan terus berkembang dengan peningkatan hingga 30%. Hal ini didukung oleh pemanfaatan perangkat seperti sensor radar dan kamera yang terhubung langsung dengan jaringan komunikasi milik Kementerian Pertahanan. Sistem ini terbukti mampu meningkatkan kemampuan deteksi dini terhadap berbagai ancaman di wilayah perbatasan serta mempercepat respons terhadap aktivitas mencurigakan atau ilegal (BSSN, 2022).

Selanjutnya, pada tahun 2023, penggunaan perangkat IoT di wilayah perbatasan laut dan udara mengalami lonjakan hingga 35%. Peningkatan ini ditandai dengan penambahan sensor cerdas untuk memantau lalu lintas kapal dan pesawat asing secara lebih akurat. Selain itu, teknologi IoT juga mulai diterapkan dalam pengawasan infrastruktur strategis guna melindungi dari ancaman fisik maupun digital yang semakin kompleks (Statista, 2023).

Penerapan AI dalam Analisis Data Intelijen dan Manajemen Risiko

Pada tahun 2020, penerapan *Artificial Intelligence* (AI) dalam diplomasi pertahanan di Indonesia masih terbatas. Fokus utama penggunaan AI saat itu adalah pada pengelolaan data intelijen, khususnya untuk analisis dan deteksi pola ancaman. Teknologi ini dimanfaatkan untuk membantu proses manajemen risiko dan prediksi potensi ancaman dengan mengolah data historis yang tersedia, sehingga memberikan dasar analitis yang lebih kuat dalam pengambilan keputusan.

Tahun 2021 mencatat peningkatan penggunaan AI sebesar 20% di sektor pertahanan. AI mulai diintegrasikan secara lebih luas dalam pengolahan data intelijen dan manajemen risiko, terutama untuk mendeteksi pola-pola yang berpotensi mengganggu stabilitas keamanan nasional. Sistem AI diterapkan dalam analisis data berbasis peringatan dini dan identifikasi pola-pola ancaman yang tidak mudah dikenali oleh metode konvensional (KPMG, 2021).

Pada tahun 2022, implementasi AI dalam diplomasi pertahanan berkembang pesat hingga mencapai 40%. Salah satu terobosan utama adalah penerapan sistem analisis prediktif oleh Kementerian Pertahanan untuk mengidentifikasi ancaman siber dan bentuk ancaman non-tradisional lainnya. AI digunakan untuk memproses data yang dikumpulkan dari berbagai sumber, termasuk perangkat IoT dan laporan intelijen, sehingga memperluas cakupan dan akurasi deteksi ancaman (Hoadley & Lucas, 2018).

Tahun 2023 menunjukkan lonjakan signifikan dalam penggunaan AI, yang mencapai 50% di sektor pertahanan. Teknologi AI digunakan secara intensif untuk menganalisis data intelijen secara real-time guna mendukung pengambilan keputusan strategis secara cepat dan tepat. Selain itu, AI juga dimanfaatkan untuk mengidentifikasi potensi serangan siber, memberikan respons otomatis terhadap ancaman, serta mengelola risiko secara proaktif demi menjaga stabilitas dan keamanan nasional (BSSN, 2023).

Integrasi AI dan IoT untuk Sistem Pertahanan Siber

Pada tahun 2020, Indonesia mulai mengintegrasikan teknologi *Artificial Intelligence* (AI) dan *Internet of Things* (IoT) ke dalam sistem pertahanan siber guna meningkatkan kemampuan deteksi terhadap serangan yang menargetkan infrastruktur kritis. Langkah ini memungkinkan

pemerintah untuk memantau dan merespons ancaman siber secara lebih efektif, seiring meningkatnya kebutuhan akan sistem pertahanan digital yang adaptif dan proaktif.

Memasuki tahun 2021, adopsi AI dalam sektor pertahanan siber menunjukkan peningkatan sebesar 25%, khususnya dalam hal deteksi dan klasifikasi ancaman siber. Sementara itu, teknologi IoT mulai dimanfaatkan secara luas untuk pemantauan jaringan dan infrastruktur strategis. Badan Siber dan Sandi Negara (BSSN) mencatat bahwa integrasi kedua teknologi ini telah meningkatkan efektivitas pengawasan dan penanggulangan terhadap berbagai potensi ancaman siber (BSSN, 2022).

Pada tahun 2022, penggunaan AI dan IoT dalam sistem pertahanan siber mengalami pertumbuhan signifikan, mencapai 35%. AI digunakan secara intensif untuk menganalisis potensi ancaman secara real-time, sedangkan IoT diandalkan dalam memantau kondisi jaringan secara berkelanjutan. Sinergi kedua teknologi ini berkontribusi pada peningkatan kemampuan manajemen insiden siber, sehingga risiko terhadap serangan yang bersifat kompleks dapat diminimalisasi (National Cyber Security Centre, 2022).

Tahun 2023 menunjukkan peningkatan lebih lanjut dalam pemanfaatan AI dan IoT, dengan fokus pada diplomasi pertahanan siber. Tingkat adopsi teknologi ini meningkat hingga 40%, mencerminkan pentingnya respons cepat dan terkoordinasi terhadap insiden siber yang melibatkan infrastruktur kritis. AI digunakan untuk menganalisis serangan secara langsung, sementara IoT memperkuat kemampuan sistem dalam melakukan pemantauan dan respons otomatis terhadap insiden, yang secara keseluruhan meningkatkan resiliensi pertahanan digital nasional (Statista, 2023).

Peningkatan Infrastruktur AI dan IoT dalam Latihan Militer dan Simulasi Strategis

Pada tahun 2020, implementasi teknologi *Artificial Intelligence* (AI) dan *Internet of Things* (IoT) dalam latihan militer di Indonesia masih tergolong terbatas, dengan fokus utama pada simulasi untuk pelatihan dan perencanaan strategis. Kendati demikian, pemanfaatan teknologi ini memberikan nilai tambah dalam menciptakan kondisi pelatihan yang lebih realistis, sehingga dapat meningkatkan kesiapan dan kapabilitas personel militer secara signifikan.

Pada tahun berikutnya, yakni 2021, penerapan AI dan IoT dalam simulasi latihan militer menunjukkan peningkatan sebesar 15% dibandingkan tahun sebelumnya. Sistem berbasis AI mulai digunakan untuk merancang skenario pelatihan yang lebih kompleks dan dinamis, sehingga mendukung kemampuan militer dalam menyesuaikan strategi terhadap beragam kemungkinan taktis di lapangan (Pramono, 2023).

Perkembangan ini terus berlanjut pada tahun 2022, dengan tingkat pertumbuhan penggunaan AI dan IoT dalam latihan militer mencapai 25%. Teknologi tersebut digunakan secara lebih luas dalam proses perencanaan operasi dan evaluasi risiko, memungkinkan analisis berbasis data yang lebih akurat. IoT turut memberikan kontribusi penting melalui pemantauan logistik dan pelacakan posisi unit secara real-time, yang meningkatkan efisiensi serta efektivitas operasional militer (Schreier, 2019).

Pada tahun 2023, penggunaan AI dan IoT dalam kegiatan latihan militer mengalami peningkatan hingga 30%. Inovasi ini difokuskan pada pengembangan simulasi real-time dan analisis risiko yang lebih mendalam, dengan skenario pelatihan yang terintegrasi penuh oleh teknologi. Pendekatan ini mempersiapkan personel militer secara lebih optimal dalam menghadapi potensi ancaman modern, serta memperkuat kapasitas pertahanan melalui pemanfaatan teknologi cerdas dalam setiap tahap latihan.

Ancaman Keamanan Siber di Era *Society* 5.0

Meningkatnya adopsi teknologi digital di Indonesia juga diikuti dengan meningkatnya ancaman siber yang menjadi tantangan utama dalam *Society* 5.0. Ancaman siber di Indonesia telah menunjukkan tren peningkatan yang signifikan dalam beberapa tahun terakhir, terutama

dalam bentuk serangan terhadap infrastruktur kritis, peretasan data, dan ransomware. Badan Siber dan Sandi Negara (BSSN) melaporkan bahwa insiden siber yang berhasil ditangani pada tahun 2022 meningkat hingga 25% dibandingkan tahun sebelumnya, dengan ancaman utama datang dari serangan siber yang menargetkan data sensitif dan infrastruktur strategis, seperti sektor energi, perbankan, dan telekomunikasi (BSSN, 2022).

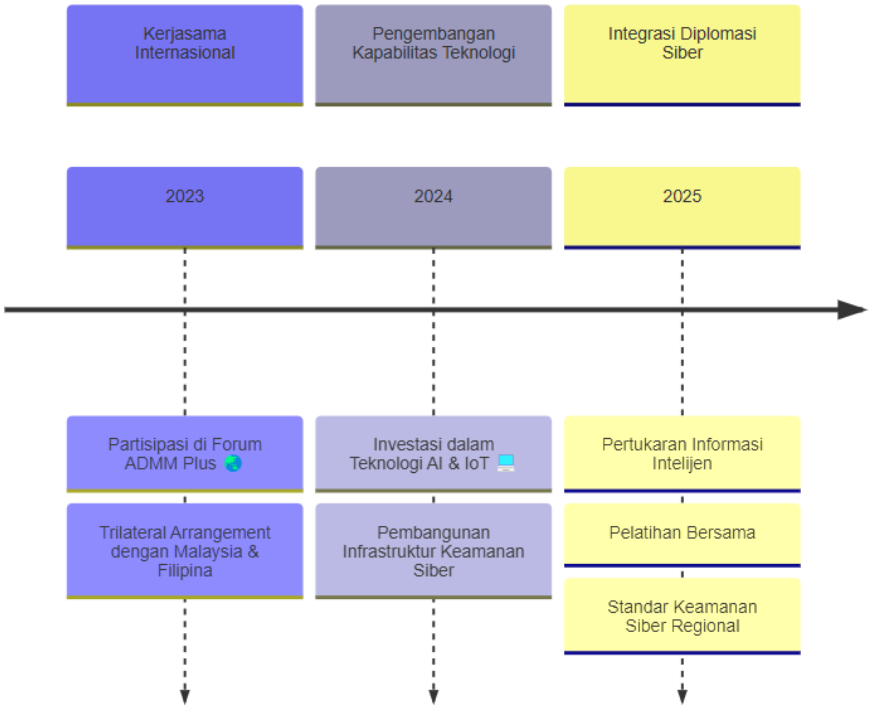
Sebagai respons terhadap meningkatnya ancaman ini, pemerintah Indonesia telah meningkatkan kebijakan keamanan siber dengan memperkuat infrastruktur digital dan membangun kerjasama internasional untuk meningkatkan kemampuan deteksi dan penanganan insiden siber. Pemerintah juga memperkenalkan regulasi terkait perlindungan data pribadi untuk meningkatkan keamanan data di sektor publik dan swasta. BSSN bekerja sama dengan berbagai lembaga internasional untuk meningkatkan kapabilitas keamanan siber melalui pelatihan, simulasi penanganan insiden siber, dan pertukaran informasi intelijen (National Cyber Security Centre, 2022). Langkah-langkah ini diharapkan dapat memperkuat ketahanan siber Indonesia dalam menghadapi ancaman di era *Society* 5.0.

Strategi Diplomasi Pertahanan yang Efektif

Dalam menghadapi tantangan *Society* 5.0, diplomasi pertahanan Indonesia memerlukan strategi kolaboratif yang melibatkan kerjasama dengan negara-negara lain untuk memperkuat pertahanan siber. Strategi diplomasi pertahanan yang efektif mencakup tiga aspek utama: peningkatan kerjasama internasional, pengembangan kapabilitas teknologi, dan integrasi diplomasi siber dalam kebijakan keamanan nasional. Pertama, kerjasama internasional menjadi penting untuk menghadapi ancaman siber yang bersifat lintas batas. Indonesia telah berpartisipasi dalam forum-forum seperti ASEAN *Defence Ministers' Meeting* (ADMM) Plus dan mengembangkan Trilateral Cooperative Arrangement dengan Malaysia dan Filipina untuk meningkatkan keamanan kawasan di Laut Sulu (Pramono, 2023).

Kedua, pengembangan kapabilitas teknologi menjadi prioritas dalam diplomasi pertahanan. Indonesia telah meningkatkan investasi dalam teknologi AI dan IoT untuk deteksi dini ancaman, serta mengembangkan infrastruktur keamanan siber untuk menjaga stabilitas dalam negeri. Penggunaan AI dan big data dalam analisis risiko dan pengambilan keputusan membantu pemerintah mendeteksi potensi ancaman dengan lebih cepat dan akurat, sementara IoT memungkinkan pemantauan infrastruktur kritis secara real-time (Schreier, 2019).

Ketiga, integrasi diplomasi siber dalam kebijakan keamanan nasional adalah langkah yang esensial untuk memperkuat pertahanan siber di era digital. Indonesia perlu mengembangkan strategi diplomasi siber yang mencakup kerja sama dalam pertukaran informasi intelijen, pelatihan bersama, serta kesepakatan untuk standar keamanan siber di kawasan. Dengan pendekatan yang kolaboratif, pemerintah dapat meningkatkan ketahanan siber nasional sekaligus memperkuat hubungan internasional, yang pada akhirnya mendukung stabilitas keamanan nasional dalam menghadapi era *Society* 5.0. Gambar 3 menunjukkan strategi diplomasi pertahanan Indonesia dalam menghadapi *Society* 5.0



Gambar 3. Strategi Diplomasi Pertahanan Indonesia dalam Menghadapi *Society* 5.0

Peluang dan Tantangan Diplomasi Pertahanan di Era *Society* 5.0

Di era *Society* 5.0, diplomasi pertahanan menghadapi berbagai peluang dan tantangan yang perlu dievaluasi baik dari sudut pandang akademis maupun praktis. Dari sudut pandang akademis, *Society* 5.0 menawarkan peluang untuk memperkuat pertahanan nasional dengan memanfaatkan teknologi digital, seperti AI, IoT, dan big data, yang dapat memberikan kemampuan prediksi dan respons yang lebih cepat terhadap potensi ancaman. Dengan adanya *Society* 5.0, diplomasi pertahanan memiliki kesempatan untuk mengembangkan strategi berbasis data yang didukung oleh analitik prediktif, pemantauan real-time, dan otomatisasi dalam pengelolaan risiko (Deguchi et al., 2020). Pendekatan berbasis teknologi ini juga memungkinkan diplomasi pertahanan untuk lebih adaptif terhadap ancaman siber yang bersifat dinamis dan kompleks.

Namun, dari perspektif praktis, *Society* 5.0 juga menghadirkan tantangan signifikan. Implementasi teknologi tinggi dalam diplomasi pertahanan membutuhkan infrastruktur digital yang kuat dan sumber daya manusia yang terampil dalam pengoperasian teknologi tersebut. Selain itu, *Society* 5.0 meningkatkan ketergantungan pada teknologi digital, yang membuka peluang bagi ancaman siber untuk mengganggu stabilitas nasional dan infrastruktur kritis. Kerentanan ini menuntut adanya kebijakan keamanan siber yang ketat serta kolaborasi internasional yang lebih intensif untuk menghadapi serangan yang bersifat lintas batas dan dilakukan oleh aktor negara maupun non-negara (Hoadley & Lucas, 2018). Tantangan ini menunjukkan bahwa meskipun *Society* 5.0 memberikan peluang bagi diplomasi pertahanan, keberhasilan implementasinya sangat bergantung pada kesiapan infrastruktur, kebijakan keamanan yang tepat, serta kemampuan diplomasi untuk menjalin kerjasama yang kuat di tingkat regional dan global.

Peran Teknologi dalam Diplomasi Pertahanan

Teknologi seperti AI, IoT, dan big data memainkan peran penting dalam memperkuat diplomasi pertahanan di era *Society* 5.0. AI, misalnya, dapat digunakan untuk menganalisis data besar dari berbagai sumber, mengidentifikasi pola yang mencurigakan, dan memberikan peringatan dini tentang potensi ancaman. Teknologi ini memungkinkan diplomasi pertahanan untuk mengantisipasi dan merespons ancaman dengan lebih cepat, serta membuat pengambilan keputusan lebih berbasis data (Schmidt & Cohen, 2019). Di samping itu, AI mendukung sistem otomatisasi dalam operasi pertahanan dan membantu dalam analisis data intelijen yang lebih mendalam dan akurat.

IoT, sebagai jaringan perangkat yang terhubung, memberikan kemampuan pemantauan dan pengawasan yang real-time. Dalam konteks diplomasi pertahanan, IoT dapat digunakan untuk memantau perbatasan, melacak pergerakan di wilayah strategis, serta mengamankan infrastruktur kritis dari potensi sabotase atau serangan siber. Dengan integrasi IoT, diplomasi pertahanan dapat memperluas jangkauan pemantauan dan meningkatkan kewaspadaan terhadap ancaman keamanan yang terjadi di wilayah yang luas (Kominfo, 2022).

Big data, di sisi lain, memungkinkan diplomasi pertahanan untuk menyimpan, mengelola, dan menganalisis data dalam jumlah besar yang dihasilkan dari berbagai sumber, seperti sensor IoT, satelit, dan data intelijen. Analisis big data memungkinkan pengenalan pola dan deteksi anomali yang bisa menjadi indikator ancaman. Dengan memanfaatkan big data, diplomasi pertahanan dapat membangun profil risiko dan strategi mitigasi yang lebih efektif, sehingga memperkuat kemampuan respons terhadap ancaman keamanan (Schreier, 2019).

Implikasi untuk Kebijakan Nasional

Adopsi *Society* 5.0 dalam diplomasi pertahanan memiliki dampak yang signifikan terhadap stabilitas dan keamanan nasional Indonesia. Implementasi teknologi tinggi dalam sistem pertahanan memerlukan pembaruan kebijakan yang mendukung perlindungan data, pengembangan infrastruktur keamanan siber, serta peningkatan kapabilitas sumber daya manusia. *Society* 5.0 tidak hanya mempengaruhi strategi pertahanan fisik tetapi juga menuntut adanya kebijakan yang mampu menghadapi ancaman siber dan menjaga ketahanan digital di tengah ancaman yang terus berkembang (BSSN, 2022).

Kebijakan nasional perlu beradaptasi dengan cepat untuk mengantisipasi perkembangan teknologi dan ancaman yang dihasilkan. Misalnya, pemerintah dapat menetapkan regulasi terkait penggunaan AI dalam diplomasi pertahanan dan bekerja sama dengan sektor swasta untuk mengembangkan standar keamanan siber yang ketat. Di samping itu, *Society* 5.0 juga menekankan pentingnya kolaborasi internasional dalam diplomasi pertahanan, yang berarti bahwa kebijakan nasional harus mengakomodasi peningkatan kerjasama dengan negara-negara lain dalam menghadapi ancaman bersama. Langkah-langkah seperti pertukaran informasi intelijen, pelatihan bersama, dan perjanjian keamanan siber akan membantu memperkuat ketahanan nasional dan menjaga stabilitas dalam negeri di era *Society* 5.0 (National Cyber Security Centre, 2022).

Secara keseluruhan, adopsi *Society* 5.0 membawa dampak luas bagi kebijakan nasional di Indonesia. Kebijakan yang adaptif dan berbasis teknologi akan menjadi kunci bagi keberhasilan diplomasi pertahanan dalam menghadapi tantangan era digital. Dengan mengintegrasikan teknologi *Society* 5.0 dan memperkuat kerjasama internasional, Indonesia dapat meningkatkan stabilitas dan keamanan nasional serta mengantisipasi potensi ancaman siber di masa depan.

Sebagai penelitian berbasis metode sekunder, studi ini memiliki keterbatasan dalam hal akses terhadap data primer yang dapat memperkuat temuan. Selain itu, analisis yang dilakukan terutama bergantung pada literatur yang tersedia, yang mungkin tidak sepenuhnya mencerminkan perkembangan terbaru dalam kebijakan pertahanan siber Indonesia.

Agenda penelitian masa depan dapat diarahkan pada beberapa fokus strategis guna memperkuat kajian dan praktik diplomasi pertahanan Indonesia di era *Society* 5.0. Pertama, diperlukan studi empiris yang secara sistematis mengevaluasi efektivitas kebijakan pertahanan siber nasional, khususnya melalui pengumpulan data primer dari wawancara maupun survei dengan para pemangku kepentingan yang terlibat secara langsung dalam perumusan dan implementasi kebijakan tersebut. Kedua, analisis perbandingan dengan negara-negara yang telah berhasil mengintegrasikan konsep *Society* 5.0 ke dalam kebijakan pertahanannya menjadi penting untuk mengidentifikasi praktik terbaik (*best practices*) yang relevan dan dapat diadaptasi. Ketiga, perlu dikembangkan suatu model strategi kebijakan berbasis teknologi dan inovasi yang dapat dijadikan acuan oleh pemerintah Indonesia dalam meningkatkan kesiapan dan respons terhadap berbagai bentuk ancaman digital. Dengan demikian, hasil penelitian ini diharapkan tidak hanya berkontribusi secara teoretis dalam pengembangan ilmu pertahanan siber, tetapi juga memberikan rekomendasi kebijakan yang konkret dan aplikatif untuk memperkuat posisi Indonesia dalam kancah diplomasi pertahanan global.

KESIMPULAN

Penelitian ini menemukan bahwa *Society* 5.0 telah mengubah paradigma diplomasi pertahanan dengan menuntut integrasi teknologi canggih seperti AI, IoT, dan big data dalam kebijakan keamanan nasional. Dalam konteks Indonesia, adopsi teknologi ini masih menghadapi tantangan berupa keterbatasan infrastruktur dan sumber daya manusia yang belum optimal. Meskipun demikian, upaya peningkatan kerja sama internasional dan penguatan regulasi keamanan siber dapat menjadi strategi yang efektif dalam mengatasi ancaman digital. Oleh karena itu, studi ini menegaskan bahwa diplomasi pertahanan yang adaptif dan berbasis teknologi merupakan kunci utama dalam menghadapi tantangan keamanan di era *Society* 5.0, serta merekomendasikan penguatan infrastruktur digital dan kolaborasi lintas negara sebagai langkah strategis ke depan.

DAFTAR PUSTAKA

Aritonang, A. A. D., & Aritonang, S. (2024). *Hubungan internasional & diplomasi*. CV. Aksara Global Akademia. ISBN: 978-623-8704-16-3.

Baldwin, D. A. (2019). *Power and international relations: A conceptual approach*. Princeton University Press. ISBN: 978-0691186644.

Bendrath, R. (2020). *AI and international security: Balancing technological advances and security*. Routledge. ISBN: 978-0367857285.

Buchanan, B. (2020). *The hacker and the state: Cyber-attacks and the new normal of geopolitics*. Harvard University Press. ISBN: 978-0674987555.

Badan Pusat Statistik (BPS). (2021). *Statistik penggunaan big data di Indonesia*. Badan Pusat Statistik.

Badan Siber dan Sandi Negara (BSSN). (2022). *Laporan keamanan siber Indonesia*. Badan Siber dan Sandi Negara.

Center for Strategic and International Studies. (2022). *Significant cyber incidents*. Retrieved from https://www.csis.org.

Deguchi, A., Ito, J., & Hirano, T. (2020). *Society 5.0: A people-centered Society*. Keio University Press.

Erdos, D. (2021). Data privacy and cybersecurity. I*nternational Journal of Cyber Law and Policy, 5*(1), 15–29.

Fukuyama, M. (2018). Society 5.0: Aiming for a new human-centered Society. *Japan Spotlight, 1*(1), 47–50.

Giannopoulos, G., Smith, A., & Schleiss, K. (2021). *The future of cybersecurity*. Cambridge University Press. ISBN: 978-1108716826.

International Telecommunication Union. (2022). *Global cybersecurity index: GCI country profiles: Indonesia*. International Telecommunication Union.

Hoadley, D. S., & Lucas, N. J. (2018). *Cyber operations and cyber warfare*. Congressional Research Service.

Hwang, J., & Seo, K. (2021). Cyber diplomacy in national security. *Asian Journal of International Security, 7*(2), 87–101.

Japan Business Federation. (2017). *Society 5.0: Co-creating the future*. Japan Business Federation.

Kemp, S. (2022). *Digital 2022: Global overview report.* We Are Social.

Klimburg, A. (2017). *The darkening web: The war for cyberspace*. Penguin Random House. ISBN: 978-1594206661.

Kementerian Komunikasi dan Informatika (Kominfo). (2022). *Laporan transformasi digital nasional*. Kementerian Komunikasi dan Informatika.

KPMG. (2021). *The future of AI in national security*. KPMG International.

Lemnios, Z., & Weisner, T. (2019). AI and national defense. *Defense Technology Review, 12*(3), 23–41.

National Cyber Security Centre. (2022). *Cyber threat report*. UK Government.

NATO Cooperative Cyber Defence Centre of Excellence. (2021). *Global cybersecurity challenges*. NATO CCDCOE.

Organisation for Economic Co-operation and Development (OECD). (2022). *Digital security in Society 5.0: Balancing innovation and privacy*. OECD Publishing.

Prakoso, L. Y. (2020). An analysis of the South China Sea conflict: Indonesia's perspectives, contexts and recommendations. *PalArch's Journal of Archaeology of Egypt/Egyptology, 17*(4), 980-990.

Prakoso, L. Y., & Taryanto, T. (2022). Implementation of "Total War" Strategy for Supporting Indonesia Navy's Defense. *International Journal of Recent Technology and Engineering, 10*(2), 112–120.

Pramono, B. (2023). *Foreign policy in the era of global change*. CV. Aksara Global Akademia. ISBN: 978-623-8704-18-7.

Rathmell, A. (2018). *Strategic cyber defense: Managing international relations*. Palgrave Macmillan. ISBN: 978-3319932481.

Schreier, F. (2019). *Cyber-security and cyber-warfare*. United Nations Institute for Disarmament Research.

Schmidt, E., & Cohen, J. (2019). *The new digital age: Reshaping the future of people, nations, and business*. Vintage Books. ISBN: 978-0307947055.

Shin, D., & Park, Y. (2020). Cybersecurity in Society 5.0. *International Journal of Security Studies, 8*(3), 321–338.

Statista. (2022). *IoT and digital transformation in Southeast Asia*. Statista Research Department.

Toshi, T. (2021). Digital diplomacy in Society 5.0. *Journal of Asian Security Studies, 4*(2), 134–145.