

Strategi Siber Indonesia dalam Kerja Sama ASEAN untuk Menjaga Kedaulatan Digital

Muh. Fadlan Alfri Jamil^{1*}, Agussalim²

^{1,2} Departemen Ilmu Hubungan Internasional, FISIP, Universitas Hasanuddin, Indonesia
fadlan1505story@gmail.com^{1*}, agus.unhas@gmail.com²

Alamat: Jl. Perintis Kemerdekaan Km.10 Tamalanrea, Makassar, Sulawesi Selatan Indonesia 90245

Korespondensi penulis: fadlan1505story@gmail.com

Abstract. *In the era of rapid digital transformation, digital sovereignty has become a strategic issue for ASEAN countries, including Indonesia. Digital sovereignty encompasses a country's ability to manage data, technological infrastructure, and information systems independently without foreign intervention. This study aims to analyze Indonesia's strategies in strengthening digital sovereignty through regional cooperation within ASEAN. A descriptive qualitative approach is employed to illustrate the dynamics of Indonesia's domestic and regional policies, with data obtained from literature studies, official government documents, and international publications related to cybersecurity. The findings indicate that Indonesia is actively developing national policies such as the Personal Data Protection Act (PDP Law), building national digital infrastructure, and launching strategic projects such as the SATRIA-1 Satellite. At the regional level, Indonesia plays an active role in forums such as the ASEAN Digital Ministers' Meeting (ADGMIN) and ASEAN-CERT, as well as initiating the establishment of the ASEAN Digital Resilience Task Force. However, significant challenges remain, including institutional fragmentation at the national level, digital infrastructure gaps, limited human resources, and varying political commitments among ASEAN member states. This study concludes that Indonesia's strategy must be accompanied by strengthened inter-agency coordination, capacity building of human resources, and harmonization of regional digital policies to create a secure, sovereign, and inclusive ASEAN digital ecosystem.*

Keywords: ASEAN, Cyber Diplomacy, Cybersecurity, Digital Infrastructure, Digital Sovereignty

Abstrak. Di era transformasi digital yang pesat, kedaulatan digital menjadi isu strategis bagi negara-negara ASEAN, termasuk Indonesia. Kedaulatan digital mencakup kemampuan suatu negara dalam mengelola data, infrastruktur teknologi, dan sistem informasi secara mandiri tanpa intervensi asing. Penelitian ini bertujuan menganalisis strategi Indonesia dalam memperkuat kedaulatan digital melalui kerja sama regional di ASEAN. Pendekatan kualitatif deskriptif digunakan untuk menggambarkan dinamika kebijakan domestik dan regional Indonesia, dengan data yang diperoleh dari studi literatur, dokumen resmi pemerintah, serta publikasi internasional terkait keamanan siber. Hasil kajian menunjukkan bahwa Indonesia aktif mengembangkan kebijakan nasional seperti UU Perlindungan Data Pribadi (UU PDP), pembangunan infrastruktur digital nasional, dan peluncuran proyek strategis seperti Satelit SATRIA-1. Di tingkat regional, Indonesia berperan dalam forum-forum seperti ASEAN Digital Ministers' Meeting (ADGMIN) dan ASEAN-CERT, serta menginisiasi pembentukan ASEAN Digital Resilience Task Force. Namun, tantangan signifikan tetap ada, seperti fragmentasi kelembagaan nasional, kesenjangan infrastruktur digital, keterbatasan sumber daya manusia, serta perbedaan komitmen politik antarnegara ASEAN. Penelitian ini menyimpulkan bahwa strategi Indonesia perlu disertai dengan penguatan koordinasi antar lembaga, peningkatan kapasitas SDM, dan harmonisasi kebijakan digital regional guna menciptakan ekosistem digital ASEAN yang aman, berdaulat, dan inklusif.

Kata kunci: ASEAN, Diplomasi Siber, Keamanan Siber, Infrastruktur Digital, Kedaulatan Digital

1. LATAR BELAKANG

Di era digital kita saat ini yang semakin terhubung dengan digital lainnya, isu kedaulatan digital telah menjadi perhatian utama bagi negara-negara internasional khususnya di Asia Tenggara, termasuk Indonesia, kedaulatan digital tidak hanya menyangkut kemampuan suatu negara dalam mengelola data dan infrastruktur teknologi secara mandiri, tetapi juga mencakup perlindungan terhadap ancaman siber lintas negara,

penyebaran disinformasi, serta intervensi digital yang dapat mempengaruhi stabilitas politik dan sosial terhadap struktur tatanan negara. Dalam konteks ini, ruang digital telah berkembang menjadi arena baru bagi pertarungan kepentingan global yang menuntut kesiapan negara untuk menjaga integritas dan kemandiriannya.

Indonesia, sebagai negara demokrasi terbesar di kawasan ASEAN dengan populasi digital yang sangat besar, sering menghadapi tantangan yang tidak ringan. Serangan siber yang masif, penyebaran hoaks, dan potensi intervensi asing dalam proses politik nasional yang merupakan ancaman nyata yang dapat menggoyahkan netralitas dan keamanan ruang digital. Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa sepanjang tahun 2022, Indonesia mengalami lebih dari 900 juta anomali lalu lintas siber, sementara Kementerian Komunikasi dan Informatika (Kominfo) mencatat bahwa 93% kasus kebocoran data disebabkan oleh lemahnya sistem keamanan siber. Hal ini menunjukkan betapa krusialnya membangun sistem pertahanan digital yang kokoh dan terintegrasi.

Untuk merespons tantangan tersebut, pemerintah Indonesia telah mengembangkan berbagai inisiatif strategis, dengan pembangunan infrastruktur digital seperti peluncuran Satelit SATRIA - 1 dan penyediaan akses internet di wilayah tertinggal, terdepan, dan terluar (3T) menjadi langkah awal menuju inklusi digital yang merata. Selain itu, pemerintah juga mendorong penggunaan teknologi *open source* sebagai bentuk pengurangan ketergantungan terhadap teknologi asing. Pembentukan Angkatan Siber TNI dan penyusunan Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) juga mencerminkan keseriusan dalam membangun kapasitas pertahanan siber nasional.

Namun, upaya tersebut belum sepenuhnya bebas dari tantangan yang ada, terjadinya tumpang tindih kewenangan antara BSSN, Kominfo, Polri, dan TNI dalam penanganan isu siber menunjukkan perlunya penataan tata kelola yang lebih terkoordinasi dan efisien. Selain itu, kekurangan tenaga profesional di bidang keamanan siber serta belum optimalnya mekanisme tanggap darurat juga menjadi hambatan dalam meningkatkan efektivitas strategi nasional.

Di sisi lain, Indonesia menyadari bahwa menghadapi ancaman siber tidak dapat dilakukan secara sendiri. Perlunya kerja sama regional, khususnya melalui ASEAN, menjadi instrumen penting untuk memperkuat ketahanan digital secara kolektif. Berbagai inisiatif seperti *ASEAN Ministerial Conference on Cybersecurity* dan *ASEAN Cybersecurity Cooperation Strategy 2021–2025* menunjukkan bahwa ASEAN tengah membangun arsitektur kerja sama siber yang terkoordinasi dan komprehensif. Dalam

kerangka ini, Indonesia berperan aktif melalui BSSN sebagai focal point, termasuk dalam pembentukan ASEAN-CERT dan perumusan standar keamanan siber lintas negara.

Komitmen Indonesia terhadap isu kedaulatan digital juga terlihat dalam pengembangan kebijakan domestik seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Selain itu, pernyataan Presiden Joko Widodo pada 2023 yang menyoroti ketergantungan pemerintah pada kartu kredit asing, serta peluncuran Kartu Kredit Pemerintah (KKP) domestik, menunjukkan perhatian negara terhadap kontrol atas layanan digital strategis.

Dengan perkembangan ekonomi digital yang sangat pesat di mana pada tahun 2022 Indonesia mencatat nilai transaksi digital sebesar USD 77 miliar atau hampir 40% dari total kawasan ASEAN, dan diproyeksikan mencapai USD 130 miliar pada 2025 kebutuhan akan sistem keamanan digital yang kuat menjadi semakin mendesak.

Berdasarkan konteks tersebut, tulisan ini bertujuan untuk menganalisis strategi Indonesia dalam menjaga kedaulatan digital melalui kerja sama ASEAN. Fokus utamanya adalah pada bagaimana langkah-langkah yang telah ditempuh Indonesia, baik di tingkat nasional maupun regional, berkontribusi terhadap penguatan ketahanan siber dan integritas digital di tengah tantangan global yang terus berkembang.

2. KAJIAN TEORITIS

Kedaulatan Digital

Kedaulatan digital adalah suatu konsep yang merujuk pada kemampuan suatu negara dalam mengatur, mengelola, dan melindungi ruang digitalnya secara mandiri tanpa adanya intervensi asing. Di era globalisasi dan revolusi digital saat ini, kedaulatan digital telah menjadi bagian dari integrasi dari kedaulatan suatu negara secara keseluruhan. Perkembangan teknologi informasi dan komunikasi telah membawa perubahan dan dampak yang besar pada sistem pemerintahan negara seperti, ekonomi, pertahanan, hingga kehidupan sosial masyarakat. Namun dampak dari kemajuan ini juga telah menghadirkan tantang yang baru dan juga kompleks berupa meningkatnya kerentanan terhadap ancaman siber di bidang digital.

Menurut Setiawan (2020), serang siber merupakan bentuk ancaman kontemporer yang dapat mengganggu stabilitas nasional dari berbagai aspek, seperti politik, ekonomi, serta pertahanan dan keamanan negara. Oleh karena itu, penting bagi negara dituntut untuk membangun sistem pertahanan digital yang kuat dan terstruktur. Adanya regulasi dan

Undang – Undang Informasi dan Transaksi Elektronik (UU ITE) serta pembentukan lembaga nasional yakni Badan Siber dan Sandi Negara (BSSN) merupakan bentuk afirmasi dan langkah pemerintah Indonesia dalam menjaga kedaulatan digital tersebut. Namun sebagaimana ditegaskan oleh Setiawan regulasi domestik saja tidak cukup untuk menjaga kedaulatan tersebut, negara juga harus melibatkan berbagai aktor- aktor yang ada termasuk sektor swasta dan masyarakat sipil dalam menciptakan keamanan digital yang komprehensif.

Keamanan Siber sebagai Dimensi Keamanan Nasional

Keamanan siber saat ini merupakan salah satu dimensi yang diakui sebagai bagian dari strategis dalam keamanan nasional. Menurut Darumaya et al. (2023), ruang siber telah menjadi domain kelima dalam pertahanan dan keamanan negara yang sejajar dengan darat, laut, udara, dan juga luar angkasa. Ancaman yang ada di ruang siber bersifat lintas batas dan sering kali dilakukan oleh aktor – aktor non – negara, seperti kelompok peretas atau organisasi kriminal siber internasional yang dapat menimbulkan kerugian besar terhadap kedaulatan suatu negara. Oleh karena itu, pentingnya bagi negara untuk terus mengembangkan strategi pertahanan siber yang tidak hanya responsif, tetapi juga adaptif dan juga kolaboratif.

Di negara Indonesia, keamanan siber telah dikelola secara terpusat oleh badan resmi negara yakni BSSN yang bertanggung jawab dalam merumuskan kebijakan dan regulasi, membangun infrastruktu, serta mengawasi implementasi di sistem keamanan digital nasional. Fungsi ini mencakup perlindungan terhadap infrastruktur informasi yang kritis dan penguatan sistem yang cepat dan tanggap insiden siber. Strategi pertahanan siber nasional Indonesia juga menekankan sinergi antarlembaga, termasuk adanya keterlibatan Tentara Nasional Indonesia (TNI), Kementerian Komunikasi dan Informatik (Kominfo), serta sektor swasta. Hal ini telah menunjukkan bahwa keamanan siber menjadi isu lintas sektoral yang memerlukan pendekatan komprehensif.

Kerja Sama Regional dalam Isu Siber

Ancaman siber yang bersifat transnasional menuntut adanya kerja sama regional dan juga internasional yang lebih erat. Dalam konteks regional Asia Tenggara, ASEAN memainkan peran penting dalam mengoordinasikan upaya – upaya kolektif bagi negara – negara anggotanya untuk menghadapi berbagai tantangan dalam keamanan digital. Kerja sama ASEAN di bidang keamanan siber bertujuan membangun norma kebersamaan,

memperkuat koordinasi kebijakan, serta meningkatkan kapasitas sumber daya manusia melalui pelatihan bersama dan pertukaran informasi intelijen.

Dalam hal ini, Indoensia terus berperan aktif melalui diplomasi siber di forum ASEAN. Strategi ini difokuskan pada peningkatan keamanan nasional, dan keterlibatan dalam penyusunan norma keamanan siber di kawasan melalui partisipasi dalam ASEAN Ministerial Conference on Cybersecurity, dan pelaksanaan program ASEAN Cybersecurity Cooperation Strategy. Pendekatan ini tidak hanya memperkuat pertahanan nasional negara, tetapi juga menciptakan solidaritas antar kawasan ASEAN dalam menghadapi ancaman siber secara kolektif.

Selain itu, kerja sama ASEAN memungkinkan negara – negara anggotanya termasuk Indonesia menutup kesenjangan kapabilitas teknis dan memperkuat solidaritas dalam menghadapi konflik di ruang siber yang berpotensi mengganggu stabilitas kawasan regional. Indonesia terus mendukung pembentukan kerangka kerja regional dalam tata kelola siber yang berdasarkan pada prinsip saling menghormati, transparansi, serta kerja sama teknis yang berkelanjutan.

Pendekatan Neoliberalisme Institusional dalam Hubungan Internasional

Untuk memahami dinamika kerja sama siber di kawasan ASEAN, teori Hubungan Internasional seperti neoliberalisme institusional memberikan kerangka analisis yang relevan. Teori ini menekankan bahwa meskipun negara sebagai aktor utama dalam sistem internasional yang anarkis, kerja sama tetap mungkin terjadi apabila terdapat institusi internasional yang menciptakan norma, mengurangi ketidakpastian, dan memfasilitasi komunikasi.

Dalam konteks kerja sama siber ASEAN, institusi regional seperti ASEAN Ministerial Meeting on Cybersecurity (AMCC) dan ASEAN Digital Masterplan 2025 berfungsi sebagai platform koordinasi kebijakan dan peningkatan kapasitas bersama. Neoliberalisme institusional mengasumsikan bahwa negara – negara bersedia bekerja sama apabila mereka menyadari adanya keuntungan bersama tanpa adanya yang mengalami kerugian antar suatu pihak dan dibantu oleh institusi yang terpercaya. Hal ini tercermin dalam strategi siber Indonesia yang aktif berpartisipasi dalam forum – forum regional demi menciptakan stabilitas dan keamanan digital di kawasan regional.

Pendekatan ini menekankan pentingnya interdependensi dan pembentukan norma bersama dalam menghadapi ancaman non – tradisional seperti kejahatan siber. Dalam hal ini, diplomasi siber yang dijalankan Indonesia merupakan wujud dari komitmen untuk

membentuk masyarakat internasional yang teratur dan damai dalam ruang digital. Dalam kerangka ini diplomasi siber merupakan instrumen yang digunakan negara untuk membangun kepercayaan, meredakan konflik, dan memperkuat stabilitas di ruang digital, sebagaimana dijelaskan oleh Hamongan dan Assegaf (2020).

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deksriptif dengan tujuan untuk menganalisis bagaimana strategi Indonesia dalam kerja sama ASEAN guna menjaga kedaulatan digital. Pendekatan ini dipilih karena mampu memberikan gambaran yang mendalam mengenai dinamika kebijakan yang ada, serta tantangan yang dihadapi oleh negara Indonesia dalam konteks regional dan juga global. Jenis penelitian ini merupakan studi kualitatif, dengan pendekatan deskriptif – analitis, tujuannya adalah untuk memahami konteks, strategi, serta implikasi kerja sama Indonesia di bidang keamanan dan kedaulatan digital dalam kerangka ASEAN. Sumber data yang digunakan dalam penelitian ini merupakan data sekunder yang dikumpulkan melalui studi pustaka (library research), meliputi Arikel ilmiah, jurnal akademik, laporan riset, publikasi organisasi internasional yang relevan dengan topik, serta dokumen – dokumen yang resmi baik dari pemerintah Indonesia, dan juga Dokumen resmi dari ASEAN terkait keamanan siber. Data dianalisis menggunakan metode analisis (content analysis) yang bertujuan untuk mengidentifikasi point – point utama dalam strategi dan kebijakan siber Indonesia. Penulis menafsirkan makna, hubungan, serta kecenderungan dalam data untuk menghasilkan pemahaman yang utuh terhadap peran Indonesia dalam memperkuat kedaulatan digital melalui kerja sama Indonesia

4. HASIL DAN PEMBAHASAN

Konsep Kedaulatan Digital dalam Konteks ASEAN

Kedaulatan digital merujuk pada kemampuan suatu negara untuk mengatur, mengelola, serta melindungi ruang digitalnya secara mandiri. Contohnya seperti, negara Singapura yang telah mengembangkan pendekatan kedaulatan digital mereka melalui kebijakan “Data Localization Exemption Framework” yang memungkinkan perlindungan data tanpa sepenuhnya membatasi aliran data dalam lintas batas tertentu. Di sisi lain, negara Vietnam menerapkan kebijakan penyimpanan data lokal dan pembentukan sistem pengawasan yang ketat terhadap aktivitas digital asing, hal ini mencerminkan fokus pada kontrol nasional yang begitu kuat. Contoh – contoh tersebut menunjukkan

bahwa adanya beragam pendekatan kedaulatan digital di kawasan ASEAN yang semuanya bertujuan untuk menjaga keamanan, privasi, dan stabilitas nasional mereka di tengah arus globalisasi digital. Dalam konteks regional ASEAN, kedaulatan digital telah menjadi semakin penting di tengah transformasi digital yang begitu cepat, meningkatnya ketegangan geopolitik, serta maraknya ancaman seperti siber lintas batas. Negara – negara di ASEAN menghadapi tantangan ini dalam menjaga kedaulatan atas kedaulatan nasional mereka, berupa data warganya, mencegah akses ilegal yang dilakukan oleh entitas/oknum asing, dan terus mengembangkan sistem hukum yang relevan di era digital saat ini.

Tantangan utama di kawasan ini termasuk, belum meratanya kapasitas infrastruktur digital, kurangnya harmonisasi regulasi antara negara tetangga, serta dominasi perusahaan teknologi global yang telah menguasai data dan platform digital. Dalam situasi ini, kedaulatan digital menjadi isu yang strategi yang tak hanya berkaitan dengan keamanan informasi, tetapi juga ekonomi, hak privasi, dan kestabilan politik nasional negara. Relevansi isu ini telah menjadi wujud dalam dokumen seperti ASEAN Digital Masterplan 2025, secara eksplisit menekankan pentingnya kedaulatan digital sebagai bagian dari agenda transformasi digital khususnya di kawasan. Oleh karena itu, kedaulatan digital tidak dapat dipisahkan dari penguatan keamanan siber dan pengembangan arsitektur digital regional yang kuat.

Kepentingan Indonesia dalam Menjaga Kedaulatan Digital

Bagi Indonesia, kedaulatan merupakan kepentingan strategis nasional yang mencakup perlindungan terhadap hak data pribadi warga negara, pengamanan infrastruktur digital vital, serta pengembangan ekonomi yang mandiri. Pemerintah Indonesia telah menekankan pentingnya regulasi yang kuat dan sistem teknologi nasional yang mampu mengurangi ketergantungan pada pihak asing. Langkah yang dilakukan seperti pengembangan *Sovereign Cloud*, pusat data domestik, dan Project Qris telah menjadi bagian dari strategi ini. Ancaman yang dihadapi Indonesia antara lain serangan siber dalam skala besar (Menurut laporan BSSN mencatat serangan siber di 2022 berjumlah 976.429.996 dengan anomali trafik paling banyak masih berasal dari aktivitas malware), penyalahgunaan data, infiltrasi sistem keuangan digital oleh aktor luar, serta dominasi sistem pembayaran internasional. Ketergantungan pada platform asing juga berpotensi mengganggu kedaulatan ekonomi dan politik. Oleh karena itu, tujuan strategis Indonesia dalam sektor digital adalah menciptakan ekosistem digital yang aman, mandiri, dan terintegrasi dengan kepentingan nasional.

Peran ASEAN dalam Isu Kedaulatan Digital

ASEAN memainkan peran penting dalam membangun kerangka kerja sama digital di kawasan Asia Tenggara. Dengan melalui inisiatif seperti ASEAN Digital Masterplan 2025 dan ASEAN Cybersecurity Cooperation Strategy, ASEAN berupaya memperkuat interoperabilitas, membangun kapasitas negara anggota, dan menciptakan norma keamanan digital bersama. Mekanisme kerja sama seperti ASEAN Digital Minsters' Meeting, ASEAN – CERT, dan ASEAN – Japa Cybersecurity Capacity Building Centre menjadi instrumen penting dalam mendukung kerja sama digital.

Namun peran ASEAN juga menghadapi keterbatasan, misalnya dalam proses harmonisasi perlindungan data pribadi, perbedaan tingkat komitmen politik antara negara ASEAN menjadi hambatan signifikan. Beberapa negara seperti Singapura dan Malaysia telah memiliki kerangka hukum perlindungan data yang komprehensif dan kompatibel dengan standar internasional seperti GDPR, sementara negara lain masih berada pada tahap awal pembentukan regulasi. Perbedaan ini menyebabkan ketimpangan dalam pelaksanaan kerja sama lintas batas dan memperlambat proses penyelarasan kebijakan digital kawasan. Perbedaan tingkat kesiapan teknologi antar negara anggota, belum harmonisnya regulasi, serta perbedaan kepentingan domestik juga menjadi tantangan dalam implementasi strategi kolektif. Meskipun demikian, ASEAN tetap menjadi platform penting di kancah internasional untuk menyuarakan kepentingan kedaulatan digital dan membangun solidaritas kawasan di Asia Tenggara.

Strategi Indonesia dalam Kerja Sama ASEAN

Indonesia berupaya menunjukkan kepemimpinan dalam kerja sama digital kawasan, sebagai contoh, Indonesia menjadi salah satu negara pengusul utama ASEAN Digital Economy Framework Agreement (DEFA) dan telah berhasil menyelaraskan sejumlah standar interoperabilitas digital dengan negara – negara seperti Thailand dan Singapura. Selain itu, pada tahun 2023, Indonesia tercatat sebagai tuan rumah ASEAN Digital Ministers' Meeting (ADGMIN) dan menyampaikan inisiatif strategi terkait perlindungan data lintas batas yang disepakati sebagai bagian dari roadmap DEFA. Keterlibatan aktif ini mencerminkan pengaruh Indonesia dalam membentuk kebijakan digital kawasan dan memperkuat solidaritas ASEAN di bidang keamanan dan kedaulatan digital. Dengan melalui berbagai inisiatif, termasuk perumusan ASEAN Digital Economy Framework Agreement (DEFA), berpartisipasi dalam AMCC, serta keterlibatan aktif dalam ASEAN CERT dan CRISP. Diplomasi digital Indonesia menekankan pentingnya

menjaga keseimbangan antara keterbukaan dan perlindungan terhadap data dan sistem domestik.

Contohnya, strategi Indonesia antara lain adalah lokalisasi data, interoperabilitas sistem pembayaran melalui QRIS lintas negara, kerja sama pertahanan siber dengan negara – negara ASEAN dan mitra luar kawasan, serta harmonisasi standar perlindungan data. Pendekatan bilateral dan multilateral ditempuh secara bersamaan untuk memastikan bahwa kerja sama regional tetap mendukung kedaulatan nasional. Indonesia juga aktif mengirimkan delegasi ke pusat – pusat pelatihan siber regional seperti AJCCBC dan ASCCE, serta memperkuat kolaborasi dengan sektor swasta global untuk membanuyn pertahanan siber nasional berbasis AI.

Evaluasi dan Tantangan

Secara umum, strategi Indonesia dalam menjaga kedaulatan digital melalui ASEAN telah menunjukkan kemajuan yang signifikan, dengan berpartisipasi aktif dalam berbagai forum regional, pembentukan kebijakan nasional seperti UU PDP, serta kerja sama dalam pengembangan infrastruktur digital menunjukkan keseriusan Indonesia dalam membangun ruang digital yang aman dan mandiri. Selain menjadi tuan rumah ADGMIN 2023, Indonesia juga berhasil memfasilitasi kesepakatan ASEAN dalam cross-border data flow yang lebih terstandarisasi melalui pembahasan ASEAN Data Management Framework dan Model Contractual Clauses untuk perlindungan data lintas batas. Dokumen ini menjadi pijakan penting untuk integrasi ekonomi digital kawasan. Indonesia juga menjadi satu-satunya negara ASEAN yang secara aktif mengusulkan pembentukan ASEAN Digital Resilience Task Force, sebuah gugus tugas regional yang bertujuan meningkatkan kesiapsiagaan dan respons cepat terhadap insiden siber kolektif. Di sisi penguatan kapasitas SDM, Indonesia menjadi salah satu pengirim delegasi terbanyak ke ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) di Thailand, dengan lebih dari 100 profesional siber Indonesia mengikuti pelatihan sejak 2021. Hal ini menunjukkan komitmen nyata dalam peningkatan kapasitas nasional melalui forum kerja sama regional.

Namun tatangannya tetap ada, seperti fragmentasi regulasi nasional, kesenjangan infrastruktur digital, keterbatasan SDM, dan perbedaan kesediaan dan komitmen para pemimpin politik di antara negara anggota ASEAN menjadi penghambat untuk mengambil tindakan guna mencapai tujuan tertentu dalam mewujudkan kerja sama digital yang solid. Selain itu, dibandingkan dengan negara – negara seperti Singapura yang lebih maju secara teknologi, Indonesia masih perlu memperkuat kapasitas internalnya agar mampu

memimpin kerja sama digital di kawasan. Dengan terus mendorong diplomasi digital, memperluas regulasi dan infrastruktur, serta memperluas kerja sama teknis dan strategis, Indonesia berpotensi menjadi motor penggerak utama dalam arsitektur kedaulatan digital ASEA di masa yang akan mendatang.

5. KESIMPULAN DAN SARAN

Di tengah meningkatnya ancaman siber lintas negara dan kompleksitas geopolitik digital global, kedaulatan digital telah menjadi prioritas strategis bagi Indonesia. Sebagai negara dengan populasi digital terbesar di Asia Tenggara, Indonesia menunjukkan komitmen yang kuat melalui berbagai kebijakan nasional dan keterlibatan aktif dalam forum-forum regional ASEAN. Strategi tersebut mencakup penguatan regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), pembangunan infrastruktur digital seperti peluncuran satelit SATRIA-1 dan pusat data domestik, serta peran diplomasi siber dalam kerangka ASEAN melalui partisipasi dalam ASEAN Digital Ministers' Meeting (ADGMIN), ASEAN-CERT, dan penyusunan Digital Economy Framework Agreement (DEFA). Meskipun demikian, Indonesia masih menghadapi tantangan besar seperti fragmentasi kelembagaan, ketimpangan infrastruktur, keterbatasan sumber daya manusia, dan perbedaan tingkat kesiapan serta komitmen antarnegara ASEAN.

Untuk menjawab tantangan tersebut, pemerintah Indonesia perlu segera memperbaiki tata kelola keamanan siber nasional dengan mengurangi tumpang tindih kewenangan antar lembaga dan membentuk pusat koordinasi yang terpadu. Selain itu, peningkatan kapasitas sumber daya manusia di bidang keamanan digital harus menjadi prioritas, termasuk melalui kerja sama dengan pusat pelatihan regional dan pengembangan teknologi keamanan berbasis kecerdasan buatan. Di tingkat regional, Indonesia dapat memimpin upaya harmonisasi regulasi perlindungan data pribadi dan interoperabilitas sistem digital antarnegara ASEAN guna mendukung integrasi ekonomi digital yang aman dan berdaulat. Diplomasi digital Indonesia juga perlu diperluas ke tingkat global untuk membangun koalisi strategis yang mendukung tata kelola ruang digital yang inklusif dan adil. Terakhir, kolaborasi antara pemerintah dan sektor non-negara seperti industri teknologi, akademisi, dan masyarakat sipil perlu diperkuat. Sinergi ini akan menciptakan inovasi kebijakan dan teknologi, mempercepat transformasi digital nasional, serta membangun sistem keamanan siber yang inklusif dan adaptif terhadap tantangan yang terus berkembang. Dengan pendekatan yang kolaboratif dan visi strategis yang jelas, Indonesia berpeluang besar menjadi motor penggerak utama dalam menciptakan ekosistem digital

kawasan yang aman, berdaulatn, dan inklusif. Indonesia memiliki potensi besar untuk menjadi pemimpin dalam arsitektur kedaulatan digital di kawasan ASEAN.

DAFTAR REFERENSI

- Abdurrohim, M. (2022). ASEAN digital masterplan: Responding cyber security dilemma in the post-Covid era. *Global Focus*, Universitas Brawijaya. <https://globalfocus.ub.ac.id/index.php/globalfocus/article/download/64/32>
- Amin, K., Paramitha, D. I., & Al Farauqi, M. D. A. (2024). Managing power rivalry: Indonesia's perspective and strategy in managing relations with China in the Indo-Pacific. *Habibie Center Publications*. <https://www.habibiecenter.or.id/img/publication/edited%20volume%202024.pdf#page=87>
- Karunia, L. A., & Fardhan, Y. M. (2020). Red, white, and secured: Observing Indonesia's cybersecurity agenda with level of analysis approach. *ResearchGate*. <https://www.researchgate.net/publication/344649656>
- Karunia, L. A., & Ramlan, Y. M. F. (2024). A house of cards: Observing the unoptimized Indonesian cyber security resilience in ASEAN context. *ResearchGate*. <https://www.researchgate.net/publication/388685084>
- Khoirunnisa, M. S., & Surya, E. A. R. (2024). Implementation of cyberspace cooperation between Indonesia and United States: Combating cyberterrorism in Indonesia. *Ilomata International Journal of Social Science*. <https://www.researchgate.net/publication/382496044>
- Okano-Heijmans, M., & Vosse, W. (2021). Promoting open and inclusive connectivity: The case for digital development cooperation. *Research in Globalization*, 3, 100059. Elsevier. <https://www.sciencedirect.com/science/article/pii/S2590051X21000265>
- Ramadhan, I., & Sumadinata, R. W. S. (2022). ASEAN consensus and forming cybersecurity regulation in Southeast Asia. *ResearchGate*. <https://www.researchgate.net/publication/363128460>
- Saputri, D. P., Surryanto, D. W., & Risman, H. (2020). Indonesian cyber diplomacy: ASEAN-Japan online cyber exercise. *Technium Social Sciences Journal*, 9, 510-520. <https://heinonline.org/hol-cgibin/get\pdf.cgi?handle=hein.journals/techssj9§ion=42>
- Subroto, A., Arnakim, L. Y., & Puspita, R. A. (2023). Digital sovereignty in Indonesia-China trade relations. *Journal of Social Science*, 4(2), 287-300. <https://jsss.co.id/index.php/jsss/article/download/454/582>
- Winata, M. D., & Saleh, A. I. (2023). Indonesia's cyber security strategy: Problems and challenges. *Proceedings of the International Joint Conference on Arts and Humanities (IJCAH 2023)*. Atlantis Press. <https://www.atlantis-press.com/article/125995563.pdf>