Socius: Jurnal Penelitian Ilmu-Ilmu Sosial
Volume 3, Issue 11, June 2026, P 561-572
E-ISSN: 3025-6704
DOI: https://doi.org/10.5281/zenodo.20810423

Transformasi Strategi Keamanan Siber Jepang dalam Menghadapi Ancaman Siber Pada Era Digital (2022–2025)

Andi Arung Dewantara Faimas Putra
Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik,
Universitas Hasanuddin, Makassar, Indonesia

ARTICLE INFO
Article history:
Received 15 June 2026
Revised 20 June 2026
Accepted 24 June 2026
Available online 23 June 2026

Keywords
Active Cyber Defense, Japan, National Security Strategy 2022, Securitization Theory, Indo-Pacific.

ABSTRACT
Abstract: This study analyzes the transformation of Japan's cybersecurity strategy in the digital era, particularly following the adoption of the 2022 National Security Strategy (NSS), which introduced the Active Cyber Defense (ACD) concept for the first time. Japan faces increasingly sophisticated and persistent cyber threats from state-sponsored actors linked to China, North Korea, and Russia, threatening its critical infrastructure, defense systems, and economic assets. Employing a qualitative approach through document analysis and comparative policy analysis, this study utilizes securitization theory from the Copenhagen School complemented by the strategic culture framework as its analytical lens. The findings reveal that Japan's cybersecurity transformation constitutes a paradigmatic shift from an exclusively passive-defensive posture to a proactive defense stance. This transformation is driven by an escalating threat environment in the Indo-Pacific, the deepening of Japan and US alliance cooperation in the cyber domain, and the strategic imperatives of the Free and Open Indo-Pacific (FOIP) vision. However, the pace of transformation remains significantly constrained by Japan's pacifist constitutional framework, domestic political hesitancy, and what scholars have termed structural "Americentrism." This study contributes to theoretical debates on the securitization of cyberspace among middle-power states and offers policy-relevant insights for Indo-Pacific cybersecurity governance.

ABSTRAK
Abstrak: Penelitian ini menganalisis transformasi strategi keamanan siber Jepang pada era digital, khususnya pasca adopsi Strategi Keamanan Nasional (*National Security Strategy*/NSS) 2022 yang untuk pertama kalinya memperkenalkan konsep *Active Cyber Defense* (ACD). Jepang menghadapi ancaman siber yang semakin canggih dan persisten dari aktor-aktor yang disponsori negara, terutama Tiongkok, Korea Utara, dan Rusia, yang menargetkan infrastruktur kritis, sistem pertahanan, dan aset ekonomi strategis Jepang. Menggunakan pendekatan kualitatif melalui analisis dokumen dan analisis kebijakan komparatif, penelitian ini menerapkan teori sekuritisasi dari Sekolah Kopenhagen yang dikombinasikan dengan kerangka budaya strategis sebagai lensa analitiknya. Temuan menunjukkan bahwa transformasi keamanan siber Jepang merupakan pergeseran paradigmatik dari postur defensif-pasif eksklusif menuju postur pertahanan proaktif, yang didorong oleh eskalasi lingkungan ancaman di kawasan Indo-Pasifik, pendalaman kerja sama aliansi Jepang dengan Amerika Serikat di domain siber, dan imperatif strategis visi *Free and Open Indo-Pacific* (FOIP). Namun, kecepatan transformasi ini masih dibatasi secara signifikan oleh kerangka konstitusi pasifis Jepang, keengganan politik domestik, dan apa yang oleh para sarjana disebut sebagai "*Americentrism*" struktural. Penelitian ini berkontribusi pada perdebatan teoretis tentang sekuritisasi siber pada negara-negara *middle power* dan menawarkan wawasan relevan untuk tata kelola keamanan siber Indo-Pasifik.

PENDAHULUAN

Transformasi domain keamanan internasional pada abad ke-21 tidak dapat dilepaskan dari meningkatnya signifikansi ruang siber sebagai arena persaingan strategis antarnegara. Berbeda dengan domain keamanan tradisional yang ada di darat, laut, dan udara, domain siber memiliki karakteristik asimetris yang memungkinkan aktor dengan kapabilitas militer konvensional terbatas sekalipun untuk melancarkan serangan yang berdampak luar biasa

*Corresponding Author
e-mail: arungdewantarafp@gmail.com

terhadap negara-negara maju secara teknologi. Perkembangan ini menempatkan keamanan siber bukan sekadar sebagai persoalan teknis manajemen risiko digital, melainkan sebagai variabel strategis yang menentukan postur keamanan nasional suatu negara dalam sistem internasional yang semakin kompetitif.

Di kawasan Indo-Pasifik, dinamika keamanan siber memperoleh lapisan geopolitik yang semakin kompleks seiring meningkatnya rivalitas antara Amerika Serikat dan Tiongkok sebagai dua kekuatan besar yang bersaing memperebutkan dominasi teknologi dan tatanan siber global. Dalam konteks ini, Jepang berada pada posisi yang strategis sekaligus rentan. Hal ini karena Jepang sebagai salah satu kekuatan teknologi terdepan di dunia, sekutu dari Amerika Serikat yang paling krusial di Asia Timur, serta negara yang berbatasan langsung dengan tiga aktor siber agresif yaitu Tiongkok, Korea Utara, dan Rusia. Kerentanan ini diperparah oleh rencana pembangunan ekonomi digital Jepang melalui *Society 5.0* yang justru memperluas permukaan serangan siber secara eksponensial.

Momentum transformatif terjadi pada Desember 2022 ketika Pemerintah Kishida mengadopsi tiga dokumen strategis secara bersamaan yakni National Security Strategy (NSS), National Defense Strategy (NDS), dan Defense Buildup Program (DBP). Matsuda menilai trilogi dokumen ini sebagai terobosan transformasional yang membawa perubahan signifikan dalam aliansi Jepang dengan Amerika Serikat (Matsuda, 2023), sementara Mochinaga secara spesifik menegaskan bahwa NSS 2022 menandai titik balik dalam sejarah keamanan dan pertahanan Jepang melalui pengadopsian konsep *Active Cyber Defense* (ACD) (Mochinaga, 2025). ACD merupakan sebuah doktrin yang memungkinkan Jepang secara *pre-emptive* menetralisir komputer penyerang sebelum serangan terjadi. Pergeseran dari postur "*exclusively defense-oriented policy*" yang selama puluhan tahun menjadi jantung kebijakan keamanan Jepang menuju postur proaktif ini adalah pergeseran yang sebelumnya tidak terbayangkan dalam tradisi keamanan pasca-perang Jepang.

Kajian akademik tentang keamanan siber Jepang telah menghasilkan sejumlah wawasan penting yang membentuk perdebatan intelektual yang dinamis. Bartlett memetakan karakter defensif eksklusif kebijakan siber Jepang sebelum 2022 dan mengidentifikasi dua faktor pembentuk utamanya yaitu meningkatnya kapabilitas siber ofensif aktor-aktor regional dan kebijakan nasional Jepang yang "*exclusively defense-oriented.*" (Bartlett, 2020). Katagiri selanjutnya mengidentifikasi tiga hambatan struktural yang mencegah Jepang mengadopsi strategi siber aktif yaitu sistem hukum yang berorientasi pertahanan pasif, kendala teknis penggunaan kekuatan siber, dan kesulitan membangun deterensi yang kredibel di domain siber (Katagiri, 2021). Studi Katagiri yang memeriksa periode 2017–2020 memperlihatkan bahwa meski terjadi perubahan dalam desain kelembagaan dan operasional, kebijakan siber Jepang tetap mempertahankan inti defensifnya dan lebih bersifat bertahap daripada perombakan secara menyeluruh (Katagiri, 2022).

Namun, analisis-analisis tersebut ditulis sebelum atau tepat pada saat perubahan paradigmatik NSS 2022 terjadi, sehingga belum dapat sepenuhnya menganalisis dampak transformasi tersebut. Osawa memberikan analisis awal tentang arah kebijakan keamanan siber baru Jepang dan mengidentifikasi tantangan hukum-regulatoris dalam implementasi ACD, tetapi fokusnya lebih pada deskripsi arah kebijakan daripada analisis proses sebab-akibat yang menjelaskan mengapa dan bagaimana transformasi terjadi (Jun, 2023) . Mochinaga menawarkan analisis yang lebih komprehensif tentang pergeseran strategis Jepang, namun belum mengintegrasikannya secara sistematis dalam kerangka teori Hubungan Internasional (Mochinaga, 2025). Kritik paling tajam datang dari Nikiporets-Takigawa yang berargumen bahwa

ambisi ACD Jepang tidak layak dilaksanakan karena kendala legislatif domestik dan ketergantungan struktural pada Amerika Serikat (Nikiporets-Takigawa, 2025).

Dengan demikian, terdapat setidaknya tiga kesenjangan penelitian yang belum terjawab secara memadai. Pertama, belum ada kajian yang secara komprehensif menganalisis proses sekuritisasi keamanan siber di Jepang menggunakan teori Sekolah Kopenhagen dalam rentang temporal yang mencakup periode sebelum dan sesudah NSS 2022. Kedua, hubungan antara budaya strategis antimilitarisme Jepang dengan dinamika transformasi menuju ACD belum dieksplorasi secara sistematis dalam kerangka analisis Hubungan Internasional. Ketiga, implikasi geopolitik transformasi kebijakan siber Jepang terhadap arsitektur keamanan Indo-Pasifik, khususnya dalam dimensi *Quadrilateral Security Dialogue* (Quad) dan aliansi Jepang–AS, belum dianalisis secara terintegrasi.

Kebaruan (novelty) penelitian ini terletak pada tiga kontribusi analitik. Pertama, integrasi teori sekuritisasi dengan kerangka budaya strategis untuk menjelaskan sekaligus membatasi transformasi keamanan siber Jepang dalam satu kerangka analitik yang koheren. Kedua, fokus temporal pada periode kritis 2022–2025 yang belum banyak diteliti secara mendalam. Ketiga, penempatan transformasi keamanan siber Jepang dalam konteks persaingan geopolitik Indo-Pasifik yang lebih luas. Penelitian ini berargumen bahwa transformasi strategi keamanan siber Jepang merupakan hasil dari proses sekuritisasi bertahap yang dipercepat oleh pergeseran dramatis dalam lingkungan ancaman eksternal, meskipun proses tersebut pada saat yang sama dibentuk sekaligus dibatasi oleh warisan budaya strategis pasifisme yang menjadi karakteristik fundamental identitas keamanan Jepang pasca-Perang Dunia II.

Berdasarkan latar belakang tersebut, rumusan masalah dalam kajian ini adalah: bagaimana dan mengapa Jepang mentransformasi strategi keamanan sibernya pada periode 2022–2025, serta apa dampaknya bagi arsitektur keamanan kawasan Indo-Pasifik? Oleh karena itu, tujuan penelitian ini adalah: (1) menganalisis faktor struktural dan kontekstual yang mendorong transformasi tersebut; (2) mengidentifikasi dimensi perubahan postur dari defensif-pasif menuju *Active Cyber Defense* (ACD); (3) mengkaji akibatnya terhadap kerja sama Jepang dengan Amerika Serikat serta keamanan Indo-Pasifik; serta (4) mengevaluasi tantangan implementasi ACD dalam kendala konstitusional dan budaya strategis domestik.

METODE PENELITIAN

Penulis dalam penelitian ini akan menggunakan pendekatan **kualitatif** dalam paradigma interpretif yang bertujuan memahami transformasi kebijakan keamanan siber Jepang dalam keseluruhan kompleksitasnya sebagai fenomena yang muncul dari interaksi antara tekanan struktural internasional, kalkulasi strategis aktor negara, dan kendala normatif-domestik yang bersifat historis. Pendekatan kualitatif dipilih karena objek kajian penelitian ini, yaitu transformasi kebijakan keamanan yang tidak dapat direduksi menjadi variabel-variabel terukur tanpa kehilangan nuansa kausal yang justru menjadi inti penjelasan ilmiahnya.

Penelitian ini dirancang sebagai **studi kasus eksplikatif** (*explanatory case study*) dengan dimensi komparatif temporal. Studi kasus dipilih karena memungkinkan analisis mendalam terhadap fenomena kontemporer dalam konteks kehidupan nyata di mana batas antara fenomena dan konteksnya tidak sepenuhnya jelas. Dimensi komparatif temporal diterapkan dengan membandingkan karakteristik kebijakan siber Jepang dalam dua periode yaitu sebelum NSS 2022 (dengan titik fokus pada 2017–2021) dan sesudahnya (2022–2025). Ini merupakan perbandingan yang memungkinkan untuk mengidentifikasi magnitude perubahan dan faktor-faktor pemicunya secara lebih tajam.

Pengumpulan data dilakukan melalui tiga jalur yang saling melengkapi. **Pertama**, analisis dokumen primer meliputi: *National Security Strategy* 2022, *National Defense Strategy* 2022, *Defense Buildup Program* 2022, *Cybersecurity Strategy* Jepang berbagai tahun (2015, 2018, 2021, 2022), dan *Defense White Paper* Jepang periode 2018–2024. Dokumen-dokumen ini merupakan artefak kebijakan yang paling otentik untuk merekonstruksi pergeseran diskursif dan substantif dalam postur keamanan siber Jepang. **Kedua**, kajian sistematis terhadap literatur akademik seperti artikel jurnal, buku, dan laporan think tank bereputasi yang diterbitkan dalam rentang 2016–2026 dan relevan dengan topik kajian. **Ketiga**, laporan institusional dari organisasi internasional terkemuka seperti CSIS, RAND Corporation, dan IISS sebagai sumber data pelengkap tentang perkembangan kapabilitas dan kebijakan siber.

Analisis data dilaksanakan secara bertahap. **Pertama**, analisis isi (*content analysis*) terhadap dokumen kebijakan untuk mengidentifikasi pergeseran konseptual, terminologis, dan substantif dalam strategi keamanan siber Jepang. Analisis ini berfokus pada pelacakan perubahan *framing* ancaman siber dari risiko teknis menuju ancaman keamanan nasional eksistensial yang merupakan indikator utama proses sekuritisasi. **Kedua**, *process tracing* untuk memetakan mekanisme kausal yang menghubungkan variabel-variabel penjelas (eskalasi ancaman eksternal, tekanan aliansi, perubahan persepsi strategis) dengan variabel dependen (transformasi kebijakan siber). **Ketiga**, analisis komparatif lintas-dokumen dan lintas-periode untuk mengukur *magnitude* dan arah perubahan kebijakan. **Keempat**, triangulasi sumber untuk memvalidasi temuan dan meminimalkan bias interpretif dari sumber tunggal.

Penelitian ini mengoperasikan dua kerangka teoretis komplementer. Kerangka primer adalah teori sekuritisasi dari Sekolah Kopenhagen (Ramich et al., 2022), yang kemudian dikembangkan oleh Balzacq melalui penekanan pada praktik dan proses sekuritisasi, bukan sekadar wacana atau narasi politik (Balzacq et al., 2016). Teori ini menjelaskan bagaimana keamanan siber direkonstruksi melalui narasi politik oleh elite kebijakan Jepang sebagai ancaman eksistensial yang memerlukan langkah-langkah luar biasa (*extraordinary measures*) di luar prosedur politik normal. Kerangka komplementer adalah budaya strategis (*strategic culture*), yang menjelaskan bagaimana warisan historis pasifisme dan antimilitarisme Jepang—yang oleh Kim dianalisis sedang bertransisi dari "antimilitarisme reaktif" menuju "antimilitarisme proaktif" membentuk batas-batas transformasi yang secara politik dan normatif dapat diterima (S. Kim, 2024). Kombinasi dua kerangka ini memungkinkan analisis yang mencakup sekaligus dinamika pendorong dan kendala transformasi.

HASIL DAN PEMBAHASAN

Lanskap Ancaman Siber terhadap Jepang: Dari Gangguan Teknis Menuju Ancaman Eksistensial

Pemahaman tentang transformasi strategi keamanan siber Jepang harus dimulai dari analisis terhadap lingkungan ancaman yang melingkupinya. Selama dua dekade terakhir, Jepang mengalami eskalasi dramatis dalam jenis, frekuensi, dan kecanggihan serangan siber yang diarahkan kepadanya. Osawa mendokumentasikan lonjakan signifikan serangan siber yang disponsori negara dalam kondisi damai, dengan tiga aktor utama yaitu Tiongkok, Korea Utara, dan Rusia. Masing-masing dari mereka memiliki karakteristik pola serangan, target prioritas, dan tujuan strategis yang berbeda namun sama-sama mengancam kepentingan nasional Jepang (Jun, 2023).

Tiongkok, melalui berbagai kelompok APT (*Advanced Persistent Threats*) yang teridentifikasi berafiliasi dengan Tentara Pembebasan Rakyat (PLA) dan Kementerian Keamanan Negara (MSS), telah secara konsisten menargetkan sektor pertahanan, teknologi, dan

pemerintahan Jepang dengan motif spionase dan pencurian kekayaan intelektual. Katagiri dalam analisisnya terhadap 112 kelompok APT yang beroperasi sepanjang tahun 2003 hingga tahun 2021 mengidentifikasi bahwa motivasi dominan aktor-aktor APT yang terkait dengan negara-negara otoriter termasuk Tiongkok adalah suplementasi kekuatan militer konvensional melalui pencurian rahasia pertahanan, perolehan keunggulan teknologi melalui spionase industri, dan persiapan operasi terhadap infrastruktur kritis (Katagiri, 2024). Dalam konteks Jepang, kelompok APT10 secara luas dikaitkan dengan intelijen Tiongkok. APT10 telah berulang kali berhasil membobol sistem keamanan berbagai organisasi publik dan swasta Jepang.

Korea Utara menghadirkan ancaman yang berbeda secara karakteristik. Mereka lebih termotivasi secara finansial dan lebih berani secara operasional. Pyongyang telah menjadikan serangan siber sebagai instrumen penting penghindaran sanksi internasional dan pengumpulan dana untuk program senjata nuklirnya. Jepang, dengan ekosistem kripto dan teknologi finansial yang maju, menjadi target bernilai tinggi. Bursa-bursa kripto Jepang telah berulang kali menjadi korban peretasan yang dikaitkan dengan kelompok Lazarus yang berafiliasi dengan Korea Utara, mengakibatkan kerugian finansial yang mencapai ratusan juta dolar. Bartlett (2020) mengidentifikasi dua skenario ancaman kritis dari perspektif keamanan nasional Jepang. Pertama, penggunaan serangan siber untuk melumpuhkan operasi Pasukan Bela Diri Jepang (*Japan Self-Defense Forces*/JSDF) dalam konteks konflik bersenjata. Kedua, serangan terhadap infrastruktur kritis sipil yang dapat mengakibatkan dampak berantai yang melumpuhkan kehidupan ekonomi dan sosial.

Kerentanan Jepang diperparah oleh ambisi modernisasi teknologinya sendiri. Meningkatnya ketergantungan JSDF pada sistem teknologi canggih termasuk pemutakhiran peralatan C4I (*Command*, *Control*, *Communications*, *Computers*, *and Intelligence*) dan integrasi sistem senjata generasi berikutnya secara ironis memperluas permukaan serangan siber yang harus dilindungi. Sebagaimana Bartlett catat, JSDF mengalami kesulitan perekrutan sehingga semakin bergantung pada teknologi untuk mengkompensasi kekurangan anggota, menciptakan pola ketergantungan teknologis yang meningkatkan paparan terhadap ancaman siber (Bartlett, 2020). Dalam konteks yang lebih luas, Mochinaga menunjukkan bahwa persaingan teknologi antara Tiongkok dan Jepang khususnya dalam domain 5G, infrastruktur serat optik, dan standar ICT (Mochinaga, 2020). Hal ini telah menjadi dimensi siber dari rivalitas geopolitik yang lebih besar di kawasan Indo-Pasifik.

Dimensi ancaman yang paling mengubah kalkulasi strategis Jepang adalah meningkatnya penggunaan serangan siber sebagai komponen dari strategi "perang hibrida" yang diperlihatkan Rusia dalam operasinya terhadap Ukraina. Meski Rusia belum secara langsung menargetkan Jepang dalam serangan siber skala besar, pengamatan Jepang terhadap cara Rusia mengintegrasikan operasi siber dengan kampanye militer konvensional di Ukraina memiliki dampak serius bagi perencanaan pertahanan Jepang. Morenchuk menganalisis bahwa invasi Rusia ke Ukraina pada Februari 2022 menjadi salah satu katalis utama bagi pemerintah Kishida untuk mengakselerasi reformasi keamanan nasional Jepang, termasuk di ranah siber (G. Kim et al., 2025).

Evolusi Kebijakan Keamanan Siber Jepang: Dari Pertahanan Pasif Menuju Active Cyber Defense

Pemahaman tentang transformasi NSS 2022 memerlukan pemetaan alu perkembangan kebijakan siber Jepang sejak awal. Ukhanova mencatat bahwa sejak awal 2000-an, pemerintah Jepang secara bertahap mengembangkan visi strategis keamanan sibernya, dimulai dari fokus pada keamanan informasi yang bersifat teknis menuju pendekatan keamanan nasional yang lebih komprehensif (Ukhanova, 2022). Namun, pendekatan kuncinya sepanjang periode ini tetaplah

defensif-reaktif. Pendekatan ini membangun ketahanan sistem, meminimalkan kerentanan, dan merespons insiden yang terjadi dan bukan mencegahnya secara proaktif.

Periode 2013–2022 menandai intensifikasi bertahap. NSS pertama Jepang pada tahun 2013 di bawah Perdana Menteri Abe mulai mengakui keamanan siber sebagai bagian tak terpisahkan dari keamanan nasional, bukan sekadar isu teknis. Pembentukan *National Security Council* (NSC) memberikan kerangka kelembagaan untuk koordinasi kebijakan keamanan yang lebih terpadu. Katagiri mendokumentasikan bahwa sepanjang 2017–2020, Jepang melakukan serangkaian reformasi signifikan dalam desain kelembagaan dan operasional keamanan sibernya termasuk ekspansi unit siber JSDF, peningkatan koordinasi sipil-militer, dan penguatan kerja sama dengan sektor swasta (Katagiri, 2022). Namun, semua ini masih berlangsung dalam bingkai sudut pandang defensif yang jarang dipertanyakan. Perubahan bersifat kumulatif dan inkremental karena revolusi konseptual belum terjadi.

Lompatan kualitatif terjadi pada Desember 2022. Mochinaga menganalisis bahwa NSS 2022 menyatakan postur pemerintah untuk *Active Cyber Defense* yang secara *pre-emptive* menetralisir komputer musuh (Mochinaga, 2025). Ini adalah sebuah formulasi yang tidak pernah ada dalam kebijakan keamanan Jepang sebelumnya dan yang secara langsung menantang interpretasi konstitusional yang selama ini berlaku. ACD sebagaimana didefinisikan dalam NSS 2022 mencakup kemampuan untuk memantau jaringan dan komunikasi secara real-time termasuk komunikasi privat (dengan dampak yang signifikan bagi hak privasi), mengidentifikasi sumber serangan dan menyusup ke sistem penyerang, serta mengambil tindakan korektif proaktif terhadap infrastruktur serangan sebelum serangan terlaksana.

Osawa mengidentifikasi bahwa adopsi ACD merupakan respons langsung terhadap pengamatan Jepang terhadap implementasi ACD oleh Amerika Serikat dan Inggris Raya. Kedua negara yang memimpin dalam penggunaan respons teknis dan kebijakan, termasuk serangan siber balik, untuk mencegah dan mengawasi atribusi ancaman siber (Jun, 2023). Dalam kerangka ini, ACD Jepang dapat dipahami sebagai upaya penyelarasan dengan standar praktik terbaik sekutu-sekutunya yang sudah lebih maju dalam hal kemampuan dan kerangka hukum operasi siber proaktif.

Reformasi kelembagaan yang menyertai NSS 2022 tidak kalah signifikannya. Kim mencatat bahwa pemerintah Kishida berkomitmen menggandakan anggaran pertahanan dalam lima tahun, termasuk investasi substansial dalam kapabilitas siber. Di tingkat operasional, ini berarti ekspansi dramatis unit siber JSDF, peningkatan rekrutmen personel dengan keahlian siber, dan pembangunan infrastruktur teknis untuk mendukung operasi ACD (G. Kim et al., 2025). Matsuda menggarisbawahi bahwa trilogi dokumen strategi 2022 bukan hanya tentang peningkatan kapabilitas material, tetapi juga tentang transformasi mental dan institusional yang memungkinkan integrasi militer Jepang dan Amerika Serikat yang jauh lebih dalam (Matsuda, 2023).

Faktor Pendorong Transformasi: Analisis Kausal Multi-Level

Transformasi sebesar ini tidak muncul dari ruang hampa. Transformasi ini merupakan hasil dari penyelarasan sejumlah faktor penjelas yang beroperasi pada level analisis berbeda. Pada level sistem internasional, Kadir mengamati bahwa ancaman militer yang berkembang dari Korea Utara dan kebijakan Tiongkok yang semakin ekspansif di kawasan menjadi tekanan sistemik yang semakin sulit diabaikan. Invasi Rusia ke Ukraina pada Februari 2022 menambahkan dimensi baru (Kadir, 2025). Rusia mendemonstrasikan secara empiris bahwa perang hibrida dengan komponen siber yang terintegrasi bukan sekadar skenario teoretis, melainkan realitas kontemporer yang dapat terjadi terhadap negara mana pun yang berbatasan dengan tetangga yang agresif.

Pada level aliansi dan kerja sama multilateral, tekanan dari Amerika Serikat dan mitra Quad memainkan peran penting. Chen menganalisis bahwa strategi keamanan siber AS di bawah pemerintahan Biden secara eksplisit menekankan penguatan kerja sama keamanan siber dengan sekutu tradisional termasuk Jepang melalui mekanisme bilateral, Quad, dan Indo-Pacific Economic Framework (IPEF) (Chen & Zhang, 2025). Vosse menunjukkan bahwa EU-Jepang juga mempererat kerja sama dalam keamanan ICT sebagai pilar tambahan dalam tatanan keamanan siber Indo-Pasifik, mencerminkan penyelarasan kepentingan antara demokrasi liberal dalam mempertahankan tatanan siber yang terbuka dan aman (Vosse, 2022). Tekanan aliansi ini menciptakan ekspektasi kapabilitas yang mendorong Jepang untuk meningkatkan kemampuan sibernya agar dapat beroperasi efektif sebagai mitra koalisi.

Pada level strategis kawasan, FOIP (*Free and Open Indo-Pacific*) yang dipromosikan Jepang memiliki dimensi siber yang fundamental. Koga berargumen bahwa tujuan utama FOIP adalah membentuk dan mengkonsolidasikan tatanan regional berdasarkan tatanan internasional berbasis aturan, yang secara implisit mencakup tatanan siber yang mencegah dominasi satu aktor (Koga, 2020). Hosoya menjelaskan evolusi FOIP dari kerja sama keamanan kuadrilateral menuju kerja sama regional komprehensif yang mencakup domain digital (Hosoya, 2019). Dalam konteks ini, transformasi keamanan siber Jepang merupakan komponen yang tidak terpisahkan dari proyeksi kepemimpinan regional Jepang yang semakin asertif.

Pada level persepsi ancaman, terjadi perhitungan ulang fundamental tentang probabilitas dan konsekuensi serangan siber skala besar. Bartlett mengidentifikasi dua faktor yang membuat Jepang sangat rentan, karena rencana ekonomi digital yang memperluas permukaan serangan, dan ketergantungan JSDF pada teknologi canggih yang menciptakan target bernilai tinggi (Bartlett, 2020). Sementara Katagiri mendokumentasikan evolusi kapabilitas APT yang terkait dengan "*big four*" (Tiongkok, Iran, Rusia, Korea Utara) menunjukkan bahwa aktor-aktor ini semakin canggih, semakin terintegrasi dengan *priority strategic* dari negara-negara otoritarian, dan semakin mampu melancarkan serangan yang melampaui ambang batas kerusakan yang dapat diterima (Katagiri, 2024).

Analisis Teoretis: Sekuritisasi dan Budaya Strategis sebagai Kerangka Penjelasan

Mengapa transformasi keamanan siber Jepang terjadi sekarang dan ada apa dengan kecepatan dan *magnitude* seperti yang terlihat? Dua kerangka teoretis yang dioperasikan penelitian ini menawarkan jawaban yang saling melengkapi.

Dari perspektif teori sekuritisasi, Balzacq mengingatkan bahwa sekuritisasi bukan sekadar tindak tutur melainkan serangkaian praktik dan proses yang melibatkan aktor, audiens, dan konteks (Balzacq et al., 2016). Dalam kasus Jepang, proses sekuritisasi keamanan siber berlangsung dalam tiga fase yang dapat diidentifikasi. Fase artikulasi (2000–2013) yang dimana elite kebijakan Jepang mulai menggunakan bahasa keamanan nasional bukan sekadar bahasa manajemen risiko teknis untuk mendeskripsikan ancaman siber. Fase legitimasi (2013–2021) yang dimana rangkaian reformasi kebijakan dan kelembagaan yang direspons positif oleh audiens yang sesuai seperti DPR, sektor swasta, publik telah membangun legitimasi bagi tindakan-tindakan keamanan yang semakin luas. Fase institusionalisasi (2022–sekarang) yang dimana sekuritisasi siber mencapai tahap di mana langkah-langkah luar biasa (*extraordinary measures*) seperti operasi proaktif ke sistem komputer asing secara formal diinstitusionalisasi dalam doktrin keamanan nasional dengan NSS 2022.

Ramich menganalisis proses sekuritisasi ruang siber dari perspektif teori masyarakat jaringan Castells dan teori sekuritisasi Buzan, menunjukkan bahwa *cyber space* telah menjadi domain politik penuh dengan posisi sentral kedaulatan digital (Ramich et al., 2022). Dalam konteks Jepang, ini berarti bahwa pertanyaan tentang siber bukan lagi pertanyaan masalah teknis

semata tentang manajemen sistem informasi, melainkan pertanyaan tentang kedaulatan, identitas nasional dalam domain digital, dan kemampuan negara untuk mempertahankan otonomi dalam lingkungan teknologi yang semakin terkontes. Lacy dan Prince mengingatkan bahwa sekuritisasi keamanan siber secara global telah menciptakan risiko "*hypersecuritization*" yang dapat mengancam prinsip-prinsip terbuka internet (Lacy et al., 2018). Pertimbangan ini juga relevan untuk mengevaluasi batas normatif ACD Jepang.

Dari perspektif budaya strategis, kontribusi Kim sangat penting. Analisisnya tentang evolusi dari "antimilitarisme reaktif" menuju "antimilitarisme proaktif" dalam budaya strategis Jepang menjelaskan mengapa transformasi terjadi pada *magnitude* dan kecepatan yang terlihat namun tidak lebih cepat dan tidak lebih radikal dari itu (S. Kim, 2024). Antimilitarisme reaktif yang mendominasi dekade-dekade awal pasca-Perang Dunia II merupakan reaksi terhadap trauma perang yang memperkuat ketakutan terhadap JSDF itu sendiri. Seiring JSDF terbukti mampu berkontribusi positif pada keamanan nasional dan internasional tanpa mengulangi kesalahan historis, antimilitarisme mengalami redefinisi menjadi kewaspadaan terhadap penggunaan kekuatan militer yang berlebihan dan bukan terhadap keberadaan kapabilitas pertahanan yang memadai. Dalam konteks siber, ini berarti masyarakat Jepang lebih reseptif terhadap kapabilitas siber defensif-proaktif sepanjang kapabilitas tersebut didefinisikan, dioperasikan, dan diawasi dalam batas-batas yang konsisten dengan nilai-nilai antimilitaristis.

Ketegangan antara proses sekuritisasi yang mendorong ekspansi kapabilitas dan budaya strategis yang membatasi laju serta *magnitude* ekspansi tersebut menjelaskan karakteristik unik transformasi keamanan siber Jepang. Hal ini dapat dilihat dari transformasi keamanan siber Jepang yang signifikan secara konseptual (ACD adalah terobosan doktrin), tetapi masih terhambat dalam implementasi praktis karena keterbatasan legislatif dan kapasitas teknis. Nikiporets-Takigawa menangkap ketegangan ini dengan jelas ketika berargumen bahwa strategi keamanan siber terbaru Jepang yang menargetkan "*active defense*" tidak layak dilaksanakan karena elite politik enggan secara mandiri dan tegas mengadopsi legislasi yang diperlukan sebuah keengganan yang mencerminkan betapa dalamnya nilai-nilai budaya strategis masih mempengaruhi pengambilan keputusan bahkan di tengah eskalasi ancaman (Nikiporets-Takigawa, 2025).

Dimensi Aliansi dan Implikasi bagi Arsitektur Keamanan Indo-Pasifik

Transformasi keamanan siber Jepang tidak dapat dipahami secara akurat tanpa menempatkannya dalam konteks aliansi dan arsitektur keamanan regional yang lebih luas. Matsuda berargumen bahwa NSS 2022 semakin mempercepat tren integrasi strategis dan institusional antara Jepang dan AS yang telah berlangsung sepanjang dekade sebelumnya (Matsuda, 2023). Dalam domain siber, integrasi ini mencakup berbagi intelijen ancaman siber yang lebih dalam, pengembangan kapabilitas pertahanan siber yang terkoordinasi, dan harmonisasi doktrin operasi siber untuk memungkinkan interoperabilitas dalam respons siber bersama.

Atanassova-Cornelis menganalisis bahwa Jepang semakin memainkan peran kepemimpinan dalam arsitektur keamanan regional yang semakin cair, melampaui sistem aliansi formal yang dipimpin oleh Amerika Serikat. Dalam konteks keamanan siber, ini termanifestasikan dalam upaya Jepang membangun jaringan kerja sama siber bilateral dengan Australia, India, dan Inggris Raya. Jepang tidak membangun jaringan kerja sama siber bilateral dengan Amerika Serikat sebagai bagian dari strategi "*webbing*" mitra keamanan yang sesuai nilai (*like-minded states*) (Atanassova-Cornelis, 2020). Murphy mengidentifikasi bahwa *middle powers* di Indo-Pasifik menemukan dua area kerja sama siber paling menjanjikan yakni *confidence-*

building measures dan *capacity-building measures* (Murphy & Nagy, 2024). Keduanya merupakan domain di mana Jepang telah aktif berperan sebagai donor dan promotor.

Dimensi FOIP memberikan kerangka geopolitik bagi transformasi ini. Satake menjelaskan bahwa FOIP, meski sering dipersepsikan sebagai strategi penahanan terhadap Tiongkok, pada dasarnya adalah strategi pembangunan tatanan yang inklusif termasuk dalam domain digital (Satake, 2019). Satake dan Hemmings lebih jauh berargumen bahwa FOIP Jepang berusaha mempertahankan tatanan regional terbuka yang menginkorporasi semua negara kawasan dalam kerangka bersama. Ketegangan antara ambisi inklusivitas ini dengan keharusan berhadapan dengan ancaman siber dari Tiongkok dan Korea Utara menciptakan dilema strategis yang nyata bagi Tokyo (Satake & Sahashi, 2021).

Mochinaga menganalisis respons Jepang terhadap perluasan *Digital Silk Road Tiongkok* sebagai persaingan di lapangan yang berbeda namun terhubung dengan standar ICT, infrastruktur serat optik, dan ekosistem teknologi 5G menjadi arena persaingan yang hasilnya akan menentukan siapa yang mengendalikan lapisan infrastruktur dari mana domain siber beroperasi (Mochinaga, 2020). Dalam persaingan ini, strategi Jepang tidak hanya defensif tetapi juga konstruktif dalam membangun alternatif infrastruktur digital yang dapat dipercaya di kawasan. Hal ini merupakan sebuah dimensi dari keamanan siber yang jauh melampaui pertahanan jaringan konvensional.

Hughes dalam analisis yang berangkat dari konteks yang lebih luas tentang kebijakan bela diri kolektif Jepang, memberikan perspektif yang berguna untuk memahami transformasi siber berupa perubahan yang dibuat oleh pemerintah Jepang disajikan sebagai "moderasi dan kontinuitas" sesungguhnya merupakan pergeseran radikal dalam arah kebijakan yang strategis (HUGHES, 2017). Dalam konteks siber, framing ini terlihat jelas dalam cara NSS 2022 mempresentasikan ACD sebagai kelanjutan logis dari prinsip bela diri yang sudah ada padahal secara secara mendasar ia merepresentasikan terobosan prinsip yang belum pernah ada sebelumnya.

Kendala Implementasi: Jurang antara Ambisi Doktrin dan Realitas Institusional

Analisis yang jujur tentang transformasi keamanan siber Jepang harus mengakui jarak yang masih signifikan antara ambisi doktriner NSS 2022 dan realitas implementasinya. Katagiri mengidentifikasi dimensi teknis dari celah ini sebagai atribusi serangan siber tetap menjadi tantangan metodologis yang sangat sulit, dan tanpa kapabilitas atribusi yang handal, justifikasi untuk tindakan ACD menjadi sangat rentan terhadap kesalahan yang berpotensi memicu eskalasi yang tidak diinginkan (Katagiri, 2021).

Dimensi hukum dari hambatan implementasi bahkan lebih fundamental. Osawa mengidentifikasi bahwa undang-undang yang berlaku di Jepang melarang akses tidak sah ke sistem komputer yang secara teknis mencakup operasi ACD terhadap *server* penyerang asing (Jun, 2023). Resolusi ketegangan ini memerlukan legislasi baru yang secara eksplisit mengotorisasi operasi ACD dalam kondisi tertentu, sebuah proses yang bergantung pada tercapainya konsensus politik domestik yang masih belum jelas. Bartlett sebelumnya telah mengidentifikasi bahwa kebijakan "*exclusively defense-oriented*" yang menjadi basis hukum JSDF secara historis telah ditafsirkan untuk melarang operasi ofensif dan meski reinterpretasi 2015 membuka celah untuk bela diri kolektif, penerapannya pada domain siber masih belum diselesaikan secara hukum (Bartlett, 2020).

Nikiporets-Takigawa memberikan analisis yang paling kritis dan sistematis tentang hambatan ini. Ia berargumen bahwa dua faktor struktural saling memperkuat untuk membuat ACD tidak layak dilaksanakan. Pertama, elite politik Jepang enggan secara mandiri mengambil keputusan legislatif yang diperlukan karena kekhawatiran tentang reaksi domestik dan internasional.

Kedua, "*Americentrism*" yang terlembaga memiliki ketergantungan yang sangat dalam pada AS sebagai penyedia keamanan eksternal yang justru mengurangi insentif untuk membangun kapabilitas siber independen yang komprehensif karena selalu ada opsi mengandalkan kapabilitas sekutu (Nikiporets-Takigawa, 2025). Argumentasi ini menarik karena menunjukkan bahwa hambatan implementasi ACD bukan sekadar masalah teknis atau hukum, melainkan masalah politik ekonomi keamanan yang lebih dalam.

SIMPULAN

Penelitian ini menyimpulkan bahwa transformasi strategi keamanan siber Jepang dalam periode 2022–2025 merepresentasikan pergeseran paradigmatik yang paling signifikan dalam sejarah kebijakan keamanan pasca-perang Jepang, kendati implementasinya masih menghadapi hambatan struktural yang substansial. Melalui integrasi teori sekuritisasi dan kerangka budaya strategis, penelitian ini berhasil menjelaskan sekaligus dinamika pendorong dan kendala transformasi yang menghasilkan karakteristik unik dari arah kebijakan keamanan siber Jepang yang ambisius secara konseptual namun perlahan secara implementatif.

Pertanyaan penelitian tentang bagaimana dan mengapa transformasi terjadi dapat dijawab sebagai berikut. Transformasi terjadi melalui proses sekuritisasi bertiga-tahap yang berlangsung selama dua dekade dari artikulasi, legitimasi, hingga institusionalisasi yang puncaknya adalah pengadopsian konsep ACD dalam NSS 2022. Transformasi ini didorong oleh konvergensi faktor sistemik (eskalasi ancaman siber dari Tiongkok, Korea Utara, dan Rusia berupa demonstrasi empiris perang hibrida di Ukraina), faktor aliansi (tekanan dan ekspektasi kapabilitas dari Amerika Serikat dan Quad), dan faktor persepsi strategis (rekalkulasi probabilitas dan konsekuensi serangan siber skala besar). Namun, kecepatan dan *magnitude* transformasi dibentuk dan dibatasi oleh budaya strategis antimilitarisme proaktif yang sedang dalam transisi, yang secara bersamaan memungkinkan perluasan kapabilitas pertahanan yang signifikan sekaligus mempertahankan batas normatif terhadap militerisasi berlebihan.

Implikasi teoretis penelitian ini adalah *twofold*. Pertama, ia menunjukkan nilai analitik dari kombinasi teori sekuritisasi dan budaya strategis untuk menjelaskan transformasi kebijakan keamanan di negara-negara dengan warisan normatif yang kuat. Hal ini merupakan sebuah kontribusi yang relevan melampaui kasus Jepang untuk studi kebijakan keamanan *middle power* secara umum. Kedua, ia menunjukkan bahwa proses sekuritisasi di era digital beroperasi dengan dinamika yang berbeda dari model Sekolah Kopenhagen yang dikembangkan untuk domain keamanan tradisional berupa ancaman siber memiliki sifat yang lebih tersembunyi, atribusinya lebih sulit, dan batas antara kondisi damai dan konflik lebih kabur—semua karakteristik ini memerlukan pengembangan teoritis lebih lanjut dalam studi sekuritisasi.

Implikasi praktis bagi arsitektur keamanan Indo-Pasifik juga signifikan. Transformasi keamanan siber Jepang memperkuat pilar teknologi dari aliansi Jepang dengan Amerika Serikat dan memberikan kontribusi substantif terhadap upaya kolektif Quad dalam membangun tatanan siber yang terbuka, aman, dan berbasis aturan di kawasan. Sekaligus, ia memperlihatkan batas dari apa yang dapat dicapai negara-negara middle power dalam memperkuat postur sibernya tanpa dukungan reformasi hukum domestik yang memadai dan kapabilitas teknis yang otonom.

SARAN

Berdasarkan temuan dan analisis penelitian ini, disampaikan rekomendasi yang ditujukan kepada tiga kelompok *stakeholder*.

Bagi pemerintah Jepang, prioritas utama adalah mempercepat reformasi legislatif yang diperlukan untuk implementasi ACD yang komprehensif dan sesuai hukum. Ini mencakup revisi

Undang-Undang tentang Larangan Akses Komputer Tidak Sah untuk memberikan kewenangan eksplisit bagi operasi defensif proaktif dalam kondisi tertentu, sambil membangun mekanisme pengawasan parlementer dan yudisial yang *robust* untuk mencegah potensi penyalahgunaan. Transparansi domestik tentang batasan dan tujuan ACD sangat kritis untuk mempertahankan dukungan publik yang diperlukan bagi keberlanjutan transformasi ini. Jepang juga perlu menginvestasikan lebih besar dalam pengembangan kapabilitas atribusi siber yang andal, karena tanpanya operasi ACD akan selalu mengandung risiko eskalasi yang tidak dapat diterima.

Bagi komunitas kebijakan Indo-Pasifik dan mitra aliansi Jepang, penelitian ini merekomendasikan pengembangan kerangka normatif bersama tentang batas-batas operasi siber defensif-proaktif yang dapat diterima dalam konteks hukum internasional. Quad saat ini telah memiliki mekanisme untuk kerja sama siber, tetapi kedalaman harmonisasi doktrin operasi siber masih perlu ditingkatkan. Mekanisme "*hotline*" krisis siber antara Jepang, Amerika Serikat, Australia, dan India serupa dengan mekanisme yang ada untuk krisis nuklir dan dapat menjadi kontribusi konkret untuk manajemen eskalasi di domain yang rawan kesalahpahaman ini.

Bagi komunitas akademik, penelitian ini membuka beberapa agenda riset yang perlu dikembangkan. Pertama, studi komparatif tentang proses sekuritisasi siber di negara-negara *middle power* lain yang memiliki warisan normatif antimilitaristik seperti Korea Selatan, Jerman, dan Australia yang akan memberikan perspektif perbandingan yang berharga untuk menilai apakah trajektori Jepang merupakan pola umum atau kasus yang benar-benar unik. Kedua, analisis longitudinal tentang dampak implementasi ACD terhadap stabilitas deterensi siber regional Jepang akan menjadi kontribusi penting seiring terkumpulnya data empiris dalam tahun-tahun ke depan. Ketiga, penelitian yang mengeksplorasi perspektif Tiongkok dan Korea Utara terhadap transformasi keamanan siber Jepang dan dampaknya terhadap perhitungan strategis mereka. Hal ini akan melengkapi gambar analitik yang saat ini masih didominasi perspektif Barat dan Jepang.

REFERENSI

Atanassova-Cornelis, E. (2020). Alignment Cooperation and Regional Security Architecture in the Indo-Pacific. *The International Spectator*, *55*(1), 18–33. https://doi.org/10.1080/03932729.2020.1712132

Balzacq, T., Léonard, S., & Ruzicka, J. (2016). 'Securitization' revisited: theory and cases. *International Relations*, *30*(4), 494–531. https://doi.org/10.1177/0047117815596590;WGROUP:STRING:PUBLICATION

Bartlett, B. (2020). Japan. *Asia Policy*, *15*(2), 93–100. https://www.jstor.org/stable/27023905

Chen, T., & Zhang, G. (2025). An Examination Of The Us-Led Minilateral Cybersecurity Alliance Against China. *BULLETIN OF THE INSTITUTE OF ORIENTAL STUDIES*, 28–52. https://doi.org/10.52837/27382702-2025.5.1-28

Hosoya, Y. (2019). FOIP 2.0: The Evolution of Japan's Free and Open Indo-Pacific Strategy. *Asia-Pacific Review*, *26*(1), 18–28. https://doi.org/10.1080/13439006.2019.1622868

HUGHES, C. W. (2017). Japan's Strategic Trajectory and Collective Self-Defense: Essential Continuity or Radical Shift? *The Journal of Japanese Studies*, *43*(1), 93–126. http://www.jstor.org/stable/26448157

Jun, O. (2023). Direction of Japan's New Cybersecurity Policy. *Asia-Pacific Review*, *30*(3), 63–78. https://doi.org/10.1080/13439006.2023.2295707

Kadir, H. D. A. (2025). JAPAN'S SHIFT FROM PACIFISM: REARMAMENT AMID SECURITY CHALLENGES. *Journal of International Studies*, *21*(1), 174–198. https://doi.org/10.32890/JIS2025.21.1.10

Katagiri, N. (2021). From cyber denial to cyber punishment: What keeps Japanese warriors from active defense operations? *Asian Security*, *17*(3), 331–348. https://doi.org/10.1080/14799855.2021.1896495

Katagiri, N. (2022). Assessing Japan's cybersecurity policy: change and continuity from 2017 to 2020. *Journal of Cyber Policy*, *7*(1), 38–54. https://doi.org/10.1080/23738871.2022.2033805

Katagiri, N. (2024). Advanced persistent threats and the "big four": State-sponsored hackers in China, Iran, Russia, and North Korea in 2003–2021. *Comparative Strategy*, *43*(3), 280–299. https://doi.org/10.1080/01495933.2024.2317251

Kim, G., Seitnur, S., & Pishchalin, V. (2025). ON POLITICAL REALISM OF JAPAN'S NEW NATIONAL SECURITY STRATEGY. *KAZAKHSTAN ORIENTAL STUDIES*, *13*(1). https://doi.org/10.63051/KOS.2025.1.141

Kim, S. (2024). *Japan's militarization: from reactive to proactive antimilitarist strategic culture*. https://doi.org/10.32657/10356/181954

Koga, K. (2020). Japan's 'Indo-Pacific' question: countering China or shaping a new regional order? *International Affairs*, *96*(1), 49–73. https://doi.org/10.1093/IA/IIZ241

Lacy, M., Prince, D., Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. *Global Discourse*, *8*(1), 100–115. https://doi.org/10.1080/23269995.2017.1415082

Matsuda, T. (2023). Japan's Emerging Security Strategy. *The Washington Quarterly*, *46*(1), 85–102. https://doi.org/10.1080/0163660X.2023.2190218

Mochinaga, D. (2020). The Expansion of China's Digital Silk Road and Japan's Response. *Asia Policy*, *15*(1), 41–60. https://www.jstor.org/stable/26891387

Mochinaga, D. (2025). Rising sun in the cyber domain: Japan's strategic shift toward active cyber defense. *The Pacific Review*, *38*(2), 370–395. https://doi.org/10.1080/09512748.2024.2384447

Murphy, T., & Nagy, S. (2024). Middle Power Cyber Security Cooperation in the Indo-Pacific: An Analysis Through the Lens of Neo-Middle Power Diplomacy. *The Journal of Intelligence, Conflict, and Warfare*, *7*(1), 1–24. https://doi.org/10.21810/JICW.V7I1.6454

Nikiporets-Takigawa, G. Y. (2025). Japan's national cyber security strategy: problem field and approach's traps. *Polis. Political Studies*, *3*(3), 162–175. https://doi.org/10.17976/JPPS/2025.03.11

Ramich, M. S., Сафетович, Р. М., Piskunov, D. A., & Андреевич, П. Д. (2022). The Securitization of Cyberspace: From Rulemaking to Establishing Legal Regimes. *Vestnik RUDN. International Relations*, *22*(2), 238–255. https://doi.org/10.22363/2313-0660-2022-22-2-238-255

Satake, T. (2019). JAPAN'S "FREE AND OPEN INDO-PACIFIC STRATEGY" AND ITS IMPLICATION FOR ASEAN. *Southeast Asian Affairs*, 69–82. https://www.jstor.org/stable/26939688

Satake, T., & Sahashi, R. (2021). The Rise of China and Japan's 'Vision' for Free and Open Indo-Pacific. *Journal of Contemporary China*, *30*(127), 18–35. https://doi.org/10.1080/10670564.2020.1766907

Ukhanova, E. (2022). Cybersecurity and cyber defence strategies of Japan. *SHS Web of Conferences*, *134*, 00159. https://doi.org/10.1051/SHSCONF/202213400159

Vosse, W. (2022). A Conceptional Broadening of the Security Order in the Indo-Pacific: The Role of EU-Japan Cooperation in ICT and Cybersecurity. *Asian Affairs*, *53*(3), 561–582. https://doi.org/10.1080/03068374.2022.2090683