Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora
Volume 4 Nomor 4 October 2025
E-ISSN : 2828-7622; P-ISSN : 2828-7630, Hal 312-323
DOI: https://doi.org/10.55606/jurrish.v4i4.6534
Available Online at: https://prin.or.id/index.php/JURRISH

Diplomasi Pertahanan Siber Indonesia: Strategi, Tantangan dan Prospek

Bintang Hafizh Setiawan[1*], Hesti Rosdiana[2], Reja[3]
[1-3] Universitas Pembangunan Nasional Veteran Jakarta, Indonesia

Jl. RS Fatmawati, Pondok Labu, Jakarta Selatan
Korespondensi penulis: 2410412187@mahasiswa.upnvj.ac.id

Abstract. *The development of information and communication technology (ICT), particularly the use of Artificial Intelligence (AI), the Internet of Things (IoT), and big data, has transformed Indonesia's national security threat landscape. Threats that previously focused on traditional military aspects have now shifted to non-traditional cyber threats, such as cyberattacks, digital espionage, and infrastructure sabotage. According to PROXSIS IT GRC data, in 2024, more than 19 million cyberattacks were recorded against websites in Indonesia. While this figure is a decrease compared to the previous year, this trend is thought to reflect a shift towards more structured and organized tactics by threat actors. In response, the Indonesian government established the National Cybersecurity Action Plan 2024–2028 as a strategic guideline. Furthermore, cyber diplomacy is being promoted through bilateral and multilateral cooperation, for example through the signing of memorandums of understanding (MoUs) with the UK and Kaspersky. This cooperation includes the exchange of intelligence information, strengthening human resource capacity, raising public awareness regarding cybersecurity, and protecting critical information infrastructure. This study uses non-traditional security theory and defense diplomacy to analyze the strategies, challenges, and prospects of Indonesia's cyber policy. The analysis demonstrates that cyber defense diplomacy plays a crucial role as an instrument for integrating technology, regulation, and international collaboration in safeguarding digital sovereignty. In addition to strengthening threat detection and mitigation capabilities, this diplomacy also builds networks of trust with partner nations, which is essential amidst the increasing complexity of global threats. Therefore, in the era of digital globalization, full of interconnections, cyber defense diplomacy serves not only as a national protection tool but also as Indonesia's contribution to global cybersecurity stability. This effort prioritizes synergy between technological innovation, law enforcement, and sustainable international cooperation.*

Keywords: *Cybersecurity, Defense Diplomacy, Indonesia, National Cybersecurity Action Plan, Strategy*

Abstrak. Perkembangan teknologi informasi dan komunikasi (ICT), khususnya pemanfaatan Artificial Intelligence (AI), Internet of Things (IoT), dan big data, telah mengubah lanskap ancaman keamanan nasional Indonesia. Ancaman yang sebelumnya berfokus pada aspek militer tradisional kini bergeser menuju ancaman siber non-tradisional, seperti serangan siber, spionase digital, dan sabotase infrastruktur. Berdasarkan data PROXSIS IT GRC, pada tahun 2024 tercatat lebih dari 19 juta serangan siber terhadap situs di Indonesia. Meski angka ini menurun dibanding tahun sebelumnya, tren ini diperkirakan mencerminkan pergeseran taktik yang lebih terstruktur dan terorganisir oleh aktor ancaman. Sebagai respons, pemerintah Indonesia menetapkan Rencana Aksi Nasional Keamanan Siber 2024–2028 sebagai pedoman strategis. Selain itu, diplomasi siber digalakkan melalui kerja sama bilateral dan multilateral, misalnya melalui penandatanganan nota kesepahaman (MoU) dengan Inggris dan Kaspersky. Bentuk kerja sama ini meliputi pertukaran informasi intelijen, penguatan kapasitas sumber daya manusia, peningkatan kesadaran publik terkait keamanan siber, serta perlindungan infrastruktur informasi kritis. Dalam kajian ini, pendekatan teori keamanan non-tradisional dan diplomasi pertahanan digunakan untuk menganalisis strategi, tantangan, dan prospek kebijakan siber Indonesia. Hasil analisis menunjukkan bahwa diplomasi pertahanan siber berperan penting sebagai instrumen untuk mengintegrasikan teknologi, regulasi, dan kolaborasi internasional dalam menjaga kedaulatan digital. Selain memperkuat kemampuan deteksi dan mitigasi ancaman, diplomasi ini juga membangun jejaring kepercayaan dengan negara mitra, yang esensial di tengah meningkatnya kompleksitas ancaman global. Dengan demikian, di era globalisasi digital yang sarat interkoneksi, diplomasi pertahanan siber bukan hanya menjadi alat perlindungan nasional, tetapi juga kontribusi Indonesia terhadap stabilitas keamanan siber global. Upaya ini mengedepankan sinergi antara inovasi teknologi, penegakan hukum, dan kerja sama internasional yang berkelanjutan.

Kata kunci: Diplomasi Pertahanan, Indonesia, Keamanan Siber, Rencana Aksi Nasional Keamanan Siber, Strategi

Received: Juni 30, 2025; Revised: Juli 15, 2025; Accepted: Agustus 10, 2025; Online Available: Agustus 12, 2025

1. LATAR BELAKANG

Perkembangan keamanan dan pertahanan internasional semakin mengalami perkembangan dan perubahan wujud implementasi dalam kehidupan nyata terlebih pasca berakhirnya Perang Dingin. Perubahan kebiasaan internasional dalam sudut pandang keamanan dan pertahanan dipengaruhi oleh berbagai faktor yang terjadi, antaranya adalah tuntutan perkembangan teknologi Informasi dan Komunikasi (ICT). Perkembangan ini menyebabkan arus globalisasi semakin tidak terbendung hingga batas batas limitasi kebiasaan nasional menjadi tidak kasat mata karena terpengaruhi kebiasaan penggunaan teknologi yang semakin masif (Rahman, 2020, 2). Masyarakat pada masa ini diperkenalkan sebagai *society* 5.0 yang diperkenalkan oleh Jepang di masa kontemporer untuk merefleksikan masyarakat yang tergabung dalam integrasi penggunaan teknologi canggih seperti *artificial intelligence* (AI), *internet of Things* (IoT), big data, dan robotika yang digunakan untuk meningkatkan kesejahteraan sosial, ekonomi, dan keamanan nasional serta internasional dengan tuntutan perubahan signifikansi dari kebiasaan keamanan tradisional yang mulai transformasi menjadi ancaman non-tradisional yang mencakup seperti serangan siber, spionase digital, dan sabotase melalui jaringan komputer dengan basis digital (Aritonang, 2020, 119).

Perkembangan transformasi pada masa kontemporer ini terus dibarengi dengan perkembangan teknologi dan internet yang semakin canggih dengan konsekuensi bahwa perbandingan penggunaan untuk kesejahteraan masyarakat dengan kepentingan beberapa kelompok yang dalam memenuhi kepentingannya cenderung menggunakan pendekatan yang berbasis kejahatan atau invasi - invasi. Data perolehan yang diambil dari PROXSIS IT GRC yang mencatat bahwa pada tahun 2024 serangan serangan siber terhadap *website* yang berbasis di Indonesia berjumlah 19.171.977 kasus yang sebenarnya jumlah ini mengalami penekanan penurunan angka serangan berbasis siber yang pada tahun lalu berjumlah 29.426.930 kasus dengan catatan bahwa penurunan ini tidak semata - mata karena penurunan alamiah, tetapi karena dipengaruhi beberapa faktor diantaranya adalah penguatan basis perlindungan, perubahan taktik penyerangan, atau karena tatanan politik global karena diplomasi (Teong, 2025).

Indonesia pada prinsipnya berada pada susunan wilayah dengan kondisi geopolitik yang kompleks dengan berbasis negara kepulauan di dalam garis lintang khatulistiwa, dalam usahanya Indonesia mempertahankan pertahanan siber negara salah satunya dengan cara metode diplomasi dengan pendekatan untuk menyusun strategi, menjawab tantangan global, dan menganalisis prospek pertahanan dalam negara yang berbasis digital. Sesuai dengan mandat yang tertera dalam peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 5 Tahun

2024 tentang Rencana Aksi Nasional Keamanan Siber 2024 - 2028 untuk memastikan bahwa keamanan siber negara secara efektif dan efisien dengan mengembangkan, memanfaatkan, dan memaksimalkan penggunaan teknologi untuk menjamin keamanan digital negara.

Dalam sudut pandang internasional diplomasi pertahanan dalam bidang siber menjadi penting untuk dilaksanakan guna mengikuti tuntutan perkembangan zaman yang ada untuk menjaga persatuan atau kedaulatan negara, terselenggaranya analisis ini adalah untuk mengetahui pendekatan dalam menyusun strategi diplomasi pertahanan siber, menjawab tantangan global dan menganalisa prospek dalam menentukan atau merumuskan kebijakan terkait dalam level nasional maupun internasional, Penelitian ini penting dilakukan untuk memahami bagaimana diplomasi pertahanan siber dapat menjadi strategi efektif dalam menjawab tantangan ancaman non-tradisional yang semakin meningkat di era digital. Diplomasi pertahanan siber dalam negara indonesia memiliki makna untuk untuk menjawab tantangan diluar batas negara yang bersifat *intangible* yang semakin marak dalam perkembangan ini, dan situasi ini juga memiliki karakteristik yang identik dengan sifat ancaman siber yang kasat mata pula (Arianto & Anggraini, 2019, 14).

Diplomasi pada umumnya dikenal juga sebagai media penyelesaian suatu perkara tanpa menempuh jalan kekerasan atau penggunaan alat militer yang memungkin negara memenuhi kepentingan nasional mereka (Waskita & Sidik, 2023, 122). Penelitian ini bertujuan untuk menganalisis pendekatan diplomasi pertahanan Indonesia dalam menghadapi ancaman siber global serta meninjau prospeknya dalam konteks hubungan internasional kontemporer dan penelitian ini menggunakan pendekatan teori keamanan non-tradisional dan teori diplomasi pertahanan untuk mengkaji dinamika keamanan siber di tingkat nasional dan global. Dengan demikian penelitian ini diharapkan dapat memberikan referensi pedoman untuk menganalisis strategi, tantangan, dan prospek arah diplomasi pertahanan siber Indonesia.

2. KAJIAN TEORITIS

Urgensi diplomasi pertahanan siber negara Indonesia menjadi sangat penting untuk menjawab tuntutan perkembangan global yang ada pada masa kontemporer yang berbasis digital, pendekatan teoritis yang tepat dapat menjamin nilai konkrit dalam penelitian yang dilakukan, dalam tajuk besar kami penjabaran teoritis dalam menjawab urgensi penelitian dapat dibagi melalui sudut pandang akademis tentang *cyber defence diplomacy* dan *cyber security cooperation*.

Cyber Defence Diplomacy

Ruang lingkup keamanan siber sebuah negara berkembang pesat hingga ke puncak perhatian global di masa kontemporer ini, pertahanan siber lebih dari sekedar melindungi dari pencurian digital saja namun menjamin intelektualitas sebuah negarawan, dan memastikan keamanan nasional melalui diplomasi siber (*Cyber Diplomacy and Cybersecurity: Guardians of the Digital Realm*, 2024). Pada fokus ini, dasar teori membahas tentang pendekatan dalam membangun dialog, kerja sama, dan pemahaman bersama yang melampaui batas negara dalam bidang pertahanan siber, yang menjadikan dasar ini bukan hanya sebagai alat politik luar negeri namun juga sebagai instrumen kebijakan negara dalam mengantisipasi perselisihan dalam dunia maya (Christou, 2024, 6).

Pendekatan teori ini akan menjadi dasar analisis dalam penelitian kami dalam meninjau dalam aspek perumusan atau penetapan strategi untuk menentukan dasar pergerakan nasional untuk memenuhi kepentingan nasional masing masing negara, serta dasar teori ini juga sebagai usaha dalam menjawab tantangan bidang digital dalam sektor pembangunan infrastruktur, sistem moneter kenegaraan, sistem pemerintahan, dan sistem pemilihan umum dalam negara demokrasi, penekanan teori *Cyber Defence Diplomacy* menjadi jawaban konkrit dalam merepresentasikan kenegaraan demokratis seperti Indonesia dalam mewujudkan pemilihan umum yang adil serta memastikan keamanan pertahanan data yang dilindungi (Bjola & Manor, 2024). Pada dasarnya *Cyber Defence Diplomacy* mengatur dalam ruang lingkup tentang rujukan diplomasi pertahanan siber yang mengedepankan dialog internasional, norma, atau mengurangi eskalasi serangan siber terhadap negara (Manantan, 2021).

Cyber Security Cooperation

Teknologi informasi dan komunikasi (TIK) sudah mencapai tahap perkembangan yang mampu melebihi batas dari daya cakupan dari suatu perindividu, TIK menghadirkan salah satu tantangan konkrit untuk keamanan global bidang siber, penilaian ancaman memprediksi bahwa serangan serangan nirmiliter kedepannya akan efektif dalam menyabotase pembangunan infrastruktur negara, usaha persemakmuran rakyat, hingga kesejahteraan ekonomi, kondisi ini merupakan konsekuensi dari pendekatan peperangan asimetris dalam bidang digital atau keamanan siber negara (Chernenko et al., 2018).

Dalam ruang lingkup internasional, kerjasama dalam bidang terkait adalah pilihan bijak bagi kedua negara, namun tidak menutup kemungkinan bahwa usaha kerja sama itu melewati proses negosiasi yang apik, niscaya kerja sama dalam bidang ini tidak terjalin, maka "Internet Federasi" menjadi jawaban dalam mengamankan komposisi internet dalam negeri yang berintegritas dengan pemantauan penuh dan efektif dari pemerintah dan badan swasta (Hill,

2015). Hubungan kerja sama internasional pada dasarnya adalah untuk mencapai tujuan bersama dengan menggabungkan SDM dan SDA dari kedua belah pihak untuk meringankan proses mencapai tujuannya, dalam bidang siber pula setiap masing masing negara memiliki kesamaan tujuan yang berakhir dengan kolaborasi dengan pihak yang memiliki kesamaan tujuan pula, kerjasama keamanan siber antara Indonesia - Inggris dalam kurun periode 2019 hingga 2028 menjadi bukti nyata bahwa kedua negara memiliki kesamaan tujuan dalam memenuhi kepentingannya dengan fokus untuk pengembangan kapasitas dalam bidang siber dengan dua program utama yaitu *Cyber Law* dan *Cyber Security Awareness* yang dimulai pada tahun 2019 (Nurdiyanto et al., 2024). Kerjasama level bilateral ini secara umum memiliki tujuan untuk mengimplementasikan kebijakan yang pada referensinya adalah untuk meningkatkan kesejahteraan masyarakat secara keseluruhan.

3. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kualitatif, yang mana dalam pendekatannya menekankan pada pemahaman atas fenomena social secara mendalam. Cresweel (2014) mendefinisikan penelitian kualitatif sebagai pendekatan untuk mengeksplorasi dan memahami makna yang diberikan oleh individua tau kelompok terhadap suatu masalah social atau kemanusiaan. Dengan pendekatan studi kasus, penelitian ini menggambarkan kompleksitas suatu situasi yang dilatarbelakangi oleh beberapa faktor. Pendekatan ini juga berfokus pada pemahaman mendalam terhadap studi kasus atau sejumlah kecil kasus dalam konteks yang nyata. (Bryman, 2012).

Teknik pengumpulan data dalam penelitian ini dilakukan dengan analisis dokumen. Analisis dokumen ini diperoleh melalui dokumen tertulis resmi dan tidak resmi seperti laporan, kebijakan, perjanjian, publikasi akademik dan lain-lain. Selain itu, penelitian ini juga menggunakan studi literatur yang merujuk pada sumber historis, arsip negara, ataupun literatur akademik terdahulu untuk mendukung analisis. (Yin, 2018).

4. HASIL DAN PEMBAHASAN

Analisis Kebijakan Luar Negeri Indonesia Dalam Menyusun Strategi Pertahanan Siber

Diplomasi antar negara dapat juga didefinisikan secara umum sebagai pengelolaan kegiatan - kegiatan suatu negara melalui hubungan - hubungan resmi yang dilakukan suatu negara dengan negara-negara lain (Wagiman & Mandagi, 2016). Diplomasi ini diimplementasikan dalam bentuk kegiatan aksi nyata yang dituangkan dalam ikatan pekerjaan yang berbasis asas dari perumusan pihak kuasa yang biasanya juga dikenal sebagai kebijakan,

kebijakan dalam penelitian ini memiliki kecenderungan terhadap kebijakan luar negeri pemerintah Indonesia untuk mendasari asas pekerjaan untuk menyusun strategi nasional guna menghadapi tantangan dan tuntutan global yang berbasis digital atau siber, Edward M. Earle dan Robert E. Osgood memasukan unsur non-militer dalam kalkulasi strategis untuk menentukan arah tindakan suatu entitas (dalam hal ini negara) dalam mengawali penggunaan strategi untuk maksud-maksud damai dan perang. (Prayuda & Sundari, 2018).

Strategi pertahanan siber Indonesia pada masa kontemporer kini masih tergolong rentan akan ancaman *hacker*, penjaminan keamanan berbasis digital juga pada saat ini di Indonesia masih tidak memiliki dasar badan hukum untuk melindungi data masyarakat di dunia maya, apalagi basis server negara Indonesia masih dominan berada di luar negeri, semarak perkembangan teknologi berbasis *artificial Intelligence* dapat menjadi peluang sekaligus ancaman besar karena sudah menjadi tren kebiasaan internasional dalam pemanfaatan *artificial Intelligence* dalam bidang militer, menjawab tantangan *artificial Intelligence* antisipasi berupa pembentukan tiga indikator strategi yang harus dilaksanakan dalam menghadapi ancaman penggunaan AI, yaitu tujuan (*ends*), fasilitas/sarana prasarana (*means*), serta cara yang ditempuh (*ways*) (Rahmatika, 2022). Penyusunan Strategi pertahanan siber negara Indonesia harus memuat materi yang implisit dan inklusif dalam perumusannya untuk mencegah segala potensi ancaman yang ada dan potensi celah hukum nasional, dan juga kapasitas hukum yang harus memuat fungsi dan tujuan dari konstitusi negara yang membahas tentang kondisi pertahanan siber negara, sesuai dengan apa yang tertera pada "Pedoman Pertahanan Siber" yang dikeluarkan oleh Menteri Pertahanan Indonesia tahun 2014 bapak Purnomo Yusgiantoro memuat tentang bahwa ada beberapa kemungkinan ancaman yang perlu ditangani dengan strategi komprehensif yang melibatkan aktor negara maupun non-negara, dalam pedoman yang dijadikan rujukan penyusunan kebijakan yang komprehensif bagi Kemhan/TNI dalam menyusun, membangun, dan mengimplementasikan sistem pertahanan siber yang kokoh. Tujuan lainnya adalah untuk menciptakan koordinasi, keseragaman kebijakan, dan kesiapsiagaan dalam menghadapi berbagai potensi serangan di dunia maya (Indonesia, 2014). Dalam sudut pandang Internasional, penyusunan strategi pertahanan siber juga bisa tercipta melalui media diplomasi antar negara, pendekatan politik antar negara memungkinkan suatu negara memiliki tapal batas perilaku terhadap negara lain,

Menurut Barrinha dan Renard, diplomasi siber (cyber diplomacy) merupakan diplomasi yang dilakukan di ranah atau domain siber dimana sumber daya diplomatik dan kinerja fungsi diplomatik digunakan untuk mengamankan kepentingan nasional terkait dengan dunia maya yang dilakukan dalam format bilateral maupun multilateral. Dalam hal ini, agenda diplomatik

yang menjadi isu utamanya mencakup isu *cyber security, cyber crime, confidence-building, internet freedom,* dan *internet governance* (Chotimah, 2019, 199). Maka dari itu perumusan kebijakan luar negeri Indonesia sebagai asas berdiplomasi dalam bidang pertahanan siber harus memuat unsur kehati - hatian dan ketelitian dalam mengikuti perkembangan zaman yang disertai dengan pemanfaatan teknologi canggih sesuai dengan kebutuhan pertahanan, dan jangan lupa bahwa unsur pengamatan kejahatan berbasis siber di dalam negeri dapat menjadi landasan untuk menjadi bahan evaluasi dalam perumusan atau pemenuhan kepentingan nasional.

Tantangan Indonesia dalam Penguatan Pertahanan Siber Negara Melalui Diplomasi

Diplomasi Digital menjadi paradigma baru dalam konsep pertahanan siber yang menawarkan peluang besar bagi Indonesia dalam panggung global, dalam masa globalisasi yang didukung oleh perkembangan teknologi informasi dan komunikasi menjadikan ranah digital tidak hanya terbatas pada instrumen diplomasi saja, melainkan mencakupi urgensi dalam menjaga stabilitas pertahanan siber negara (Lumintosari et al., 2024).

Diplomasi antar beberapa negara pada fokus ini digunakan sebagai fasilitas bertukar informasi, negosiasi, dan pertukaran intelijen antar negara untuk penguatan pertahanan siber, konsep ini selaras dengan kondisi Indonesia yang masih memiliki pertahanan digital yang lemah (Anshori, 2020), Maka dari itu penguatan kapasitas pertahanan siber Indonesia menjadi urgensi untuk dijadikan prioritas pembangunan nasional guna menjawab tuntutan global di masa kontemporer, Menurut catatan dari IT PROXSIS GROUP yang merupakan badan konsultan digitalisasi swasta mencatat bahwa terdapat 19.171.977 kasus peretasan yang dihadapi Indonesia sepanjang tahun 2024, angka ini sebenarnya merupakan penurunan kasus dibanding pada tahun 2023, namun tren ini dianalisa bukan karena pertahanan digital yang semakin berkembang bagi Indonesia, tetapi merupakan persiapan akan serangan yang berskala besar, Indonesia tidak masuk dalam daftar serangan, atau perubahan taktik penyerangan, dengan kata lain bahwa prediksi serangan siber kedepannya akan semakin terorganisir dan semakin berbahaya. Untuk mencegah hal tersebut terjadi Indonesia harus mengambil langkah tegas dan serius dalam mengembangkan pertahanan siber negara baik dalam infrastruktur, kebijakan, dan implementasi di level nasional dan internasional untuk menjawab tantangan global dalam bidang keamanan dan pertahanan siber negara.

Dalam bidang penguatan kapasitas teknologi siber Kaspersky mengidentifikasikan permasalahan yang diprediksi akan eksis di masa yang akan datang, dilansir dari catatan *press release* mereka bahwa terdapat ancaman baru dalam bidang siber yaitu (1) *Offline Malware Attacks,* serangan ini pada dasarnya menggunakan perangkat keras seperti USB untuk

mengeksploitasi perangkat lunak yang berada dalam komputer, dengan memanfaatkan kerentanan keamanan komputer yang lemah serangan ini berpotensi menjadi sarana spionase, pengaksesan tanpa izin, dan sabotase perangkat (Microsoft, n.d.). (2) *P8 attack framework,* pada dasarnya serangan ini memiliki kemiripan dengan serangan *Offline Malware Attacks,* perbedaannya adalah sistematika penyusupan virus melalui basis *online* yang mempengaruhi USB pada komputer yang ditanamkan dalam bentuk kode (Kaspersky, 2021). (3) *Advanced Persistent Threats* (*APT*), APT merupakan serangan fatal yang menargetkan, mengarahkan, dan berkelanjutan pada suatu target sasaran, tujuan dari serangan ini tidak hanya terbatas pada kerusakan sistem komputer melainkan berfokus pada pencurian, manipulasi, dan pengaksesan diam diam yang biasanya berlangsung untuk jangka waktu yang lama, serangan ini biasanya dilancarkan oleh aktor besar seperti negara, NGO, hingga kelompok kriminal siber internasional, dalam melancarkan aksi ini dibutuhkan peralatan teknologi canggih yang Menggunakan teknik: *zero-day exploits*, *malware custom*, teknik pengelakan (*evasion*), dan enkripsi (MITRE, 2024).

Pertahanan siber juga selain bisa diantisipasi melalui pengembangan kapasitas teknologi juga bisa dimitigasi melalui jalur diplomasi atau kerja sama baik dengan sesama negara atau dengan NGO dalam bidang tersebut, usaha ini sesuai dengan yang tertera dalam nota kesepahaman Badan Siber dan Sandi Negara (BSSN) dengan lembaga Kaspersky untuk pengembangan kapabilitas keamanan siber di Indonesia yang ditandatangani pada 21 Juni 2021 lalu, ada pula kerjasama kenegaraan yang dilakukan Indonesia dengan Inggris pada tahun 2018 dengan ditandainya *Memorandum of Understanding* (MoU) yang ditandatangani Kepala BSSN Hinsa Siburian dan Wakil Perdana Menteri Inggris Raya Oliver Dowden di Kantor BSSN (jurnal security, 2023) yang memuat tentang substansial kerjasama kedua negara dengan ruang lingkup; (1) pertukaran informasi dan strategi (2) manajemen insiden siber (3) peningkatan kapasitas sumber daya manusia (4) kesadaran publik dan literasi siber (5) kerjasama antar pemerintah dan swasta (6) perlindungan infrastruktur kritis (7) penanggulangan kejahatan siber (8) riset dan inovasi teknologi keamanan siber (BSSN, 2018). Kerja sama ini merupakan bukti bahwa dalam penguatan unsur pertahanan negara dapat dilakukan dalam multi dimensi.

Prediksi Prospek Kerjasama Internasional bidang Pertahanan Siber di Indonesia

Indonesia yang berprinsipkan Bebas Aktif memiliki keleluasaan lebih dalam menentukan sikap permasalahan maupun kepentingan dari negara lain tanpa berpihak pada blok - blok kekuatan tertentu, prinsip ini juga mengartikan bahwa Indonesia selalu berjuang untuk mewujudkan "kemerdekaan" dan perdamaian dunia serta memenuhi kepentingan nasional negara (Haryanto, 2014). Usaha pemenuhan kepentingan nasional dalam

mempertahankan kekuatan siber negara telah mencapai tahap kerjasama yang melewati batas kedaulatan negara semata mata hanya untuk memperkuat pertahanan siber dan membangun harmonisasi antara negara terkait, kerjasama internasional adalah suatu usaha untuk memenuhi kebutuhan nasional terhadap masyarakat umum dan untuk negara - negara di dunia yang diusahakan oleh peran negara melalui kolaborasi dengan negara lain (Bagaskara, 2018).

Indonesia memiliki dasar hukum tersendiri yang menjadi pedoman dalam melakukan kerjasama dengan negara lain dalam bidang siber, sesuai dengan yang tertuang dalam Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 tahun 2014 tentang Pedoman Pertahanan Siber, dalam BAB 3 point 3.4 tentang tugas, peran, dan fungsi Pertahanan siber, Kementerian Pertahanan Mendorong partisipasi aktif dalam pemanfaatan ruang siber yang aman melalui kerjasama kemitraan nasional dan internasional lintas sektoral, dalam BAB 4 tentang Penyelenggaraan Pertahanan Siber dikuatkan bahwa Kebijakan strategis pertahanan siber Kemhan/TNI memuat unsur kebijakan kerjasama luar negeri (Kementerian Pertahanan Republik Indonesia, 2014). Pedoman tersebut menjadikan dasar bahwa masa depan pertahanan siber telah terjamin dengan salah satu usaha nya menggaet kerjasama internasional, perjanjian antara Indonesia dengan Inggris yang sudah mencapai tahap lanjutan dari perjanjian kerja sama di level bilateral. Dalam sudut pandang kerjasama dengan non-negara juga pemerintah Indonesia melakukan kerjasama dengan lembaga keamanan digital swasta yaitu Kaspersky yang diwakili oleh Badan Siber dan Sandi Negara (BSSN).

Dua bukti kerjasama ini menjadi acuan prospek kerjasama internasional bidang siber pada negara kita, mengingat Indonesia turut aktif dalam berbagai forum internasional dalam bidang pertahanan, salah satu yang menjadi pusat perhatian pada waktu dekat ini adalah keberlangsungan pameran Indo Defence 2025 Expo & Forum Gelar Defence Technology Forum yang digelar pada 12 Juni 2026 menjadi wajah bahwa komoditas pertahanan Indonesia siap untuk mengikuti perkembangan pertahanan baik di dimensi digital atau dimensi fisik, semangat perkembangan ini direfleksikan dengan pengangkatan tema topik pembahasan yaitu *Asymmetric Warfare Technology dan Advancement in Cyber Warfare.* Forum pameran tersebut dapat kita kategorikan sebagai ajang dalam memperkenalkan kekuatan militer kita dengan pendekatan *Soft Power Diplomacy*, hal ini menjadi dasar yang kuat dalam memprediksi arah perkembangan teknologi pertahanan siber kita yang dicapai dengan usaha memperkuat kapasitas pertahanan siber oleh lembaga dalam negeri dan pelebaran kerjasama militer digital melalui kerjasama internasional hasil diplomasi, hal ini

dilakukan untuk memperkuat pertahanan siber Indonesia dan mempertahankan eksistensi keaktifan Indonesia dalam partisipasi global bidang pertahanan dan perkembangan teknologi siber dunia.

5. KESIMPULAN DAN SARAN

Kesimpulan dari tulisan ini menyoroti betapa pentingnya diplomasi pertahanan siber bagi Indonesia dalam menghadapi ancaman siber yang semakin canggih dan beragam. Seiring dengan perkembangan teknologi dan globalisasi, ancaman terhadap keamanan nasional tidak hanya berasal dari serangan militer, tetapi juga dari serangan siber yang dapat mengganggu stabilitas ekonomi, pemerintahan, dan infrastruktur kritis. Dalam konteks ini, Indonesia harus memperkuat pertahanan sibernya melalui pengembangan kapasitas teknologi, peraturan yang jelas, serta kerja sama internasional yang strategis. Diplomasi pertahanan siber Indonesia berperan penting untuk melindungi kepentingan nasional, baik di tingkat domestik maupun global.

Dengan pendekatan yang tepat, diplomasi ini dapat membantu Indonesia membangun dialog, kerja sama, dan pemahaman bersama dengan negara lain, sehingga dapat mengurangi eskalasi serangan siber dan meningkatkan keamanan dunia maya. Kerja sama internasional dengan negara-negara seperti Inggris dan lembaga-lembaga swasta seperti Kaspersky telah memberikan contoh nyata bagaimana kolaborasi di bidang siber dapat memperkuat kapasitas pertahanan Indonesia. Strategi pertahanan siber Indonesia juga harus didukung oleh kebijakan yang komprehensif dan koordinasi antar lembaga negara. Hal ini mencakup penguatan infrastruktur digital dalam negeri, pembentukan regulasi yang lebih tegas terkait perlindungan data pribadi, serta peningkatan kesadaran publik dan kapasitas sumber daya manusia dalam menghadapi ancaman siber. Selain itu, Indonesia harus terus memanfaatkan forum internasional dan pameran teknologi untuk memperkenalkan kemampuan pertahanan digitalnya dan memperkuat diplomasi pertahanan siber di dunia internasional. Dengan demikian, diplomasi pertahanan siber menjadi elemen kunci dalam menjaga kedaulatan negara, melindungi masyarakat dari ancaman digital, dan memperkuat posisi Indonesia dalam tatanan global di era digital.

DAFTAR REFERENSI

Anshori. (2020, Agustus). Diplomasi digital sebagai dampak pandemi global Covid-19: Studi kasus diplomasi Indonesia di Perserikatan Bangsa-Bangsa (PBB). *Jurnal Ilmu Hubungan Internasional, 3*(2), 100–119. https://doi.org/10.33822/mjihi.v3i1.1940

Aritonang, A. A. (2020, April). Society 5.0: A people-centered society. *Jurnal Praksis dan Dedikasi, 8*(1), 119.

Badan Siber dan Sandi Negara. (2018, Juni 15). *BSSN tandatangani nota kesepahaman kerjasama di bidang keamanan siber dengan pemerintah Inggris Raya*. https://www.bssn.go.id/bssn-tandatangani-nota-kesepahaman-kerjasama-di-bidang-keamanan-siber-dengan-pemerintah-inggris-raya

Bagaskara, A. M. (2018). Kerjasama pemerintah Indonesia dan ECPAT dalam menangani permasalahan *child trafficking* di Indonesia. *Journal of International Relations, 4*(3), 367–375.

Bjola, C., & Manor, I. (Eds.). (2024). *The Oxford handbook of digital diplomacy*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780192859198.001.0001

Carter, A. B., Perry, W. J., & Steinbruner, J. D. (1992). *A new concept of cooperative security*. Bloomsbury Academic.

Chernenko, E., Demidov, O., & Lukyanov, F. (2018, Februari 27). Increasing international cooperation in cybersecurity and adapting cyber norms opinions. *Russia in Global Affairs*. https://eng.globalaffairs.ru/articles/increasing-international-cooperation-in-cybersecurity-and-adapting-cyber-norms/

Chotimah, H. C. (2019, November). Tata kelola keamanan siber dan diplomasi siber Indonesia di bawah kelembagaan Badan Siber dan Sandi Negara. *Jurnal Politica, 10*(2), 119. https://doi.org/10.22212/jp.v10i2.1447

Christou, G. (2024). *Cyber diplomacy: From concept to practice* (14th ed.). Tallinn Papers. https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_Practice_Christou.pdf

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.

Cyber diplomacy and cybersecurity: Guardians of the digital realm. (2024, Juli 16). *IE University*. https://www.ie.edu/uncover-ie/cyber-diplomacy-and-cybersecurity-guardians-of-the-digital-realm/

Haryanto, A. (2014, Desember). Prinsip bebas aktif dalam kebijakan luar negeri Indonesia: Perspektif teori peran. *Jurnal Ilmu Politik dan Komunikasi, 4*(11). https://doi.org/10.18196/hi.2015.0074.136-147

Hill, R. (2015). Dealing with cyber security threats: International cooperation, ITU, and WCIT. https://doi.org/10.1109/CYCON.2015.7158473

Jurnal Security. (2023, Juni 28). Indonesia-Inggris Raya kerjasama keamanan siber. *Jurnal Security – Media Satpam Indonesia*. https://jurnalsecurity.com/indonesia-inggris-raya-kerjasama-keamanan-siber

Kaspersky. (2021, November 28). *A new attack on secure USB drives: Kaspersky reveals key trends in the Q3 APT report*. https://www.kaspersky.com/about/press-releases/a-new-attack-on-secure-usb-drives-kaspersky-reveals-key-trends-in-the-q3-apt-report

Kementerian Pertahanan Republik Indonesia. (2014, Oktober 17). *Peraturan Menteri Pertahanan Republik Indonesia nomor 82 tahun 2014: Pedoman pertahanan siber*. https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf

Lumintosari, F. R., Santoso, M. T., & Hakiem, F. N. (2024). Peluang dan tantangan diplomasi digital dalam meningkatkan keamanan siber Indonesia. *Innovative: Journal of Social Science Research, 4*(3), 746–754. https://doi.org/10.31004/innovative.v4i3.10537

Manantan, M. B. (2021, Mei 13). Advancing cyber diplomacy in the Asia Pacific: Japan and Australia. *Australian Journal of International Affairs, 75*. https://doi.org/10.1080/10357718.2021.1926423

Microsoft. (n.d.). *How malware can infect your PC*. Microsoft Support. https://support.microsoft.com/en-us/windows/how-malware-can-infect-your-pc-872bf025-623d-735d-1033-ea4d456fb76b

MITRE. (2024, Juli 9). *APT41 DUST*. MITRE ATT&CK. https://attack.mitre.org/campaigns/C0040/

Nurdiyanto, R. A., Subagyo, A., & Sari, S. (2024). Kerjasama keamanan siber Indonesia-Inggris pada periode 2018–2028. *Mahasiswa Magister Hubungan Internasional, 1*(1), 339–349. https://doi.org/10.36859/dgsj.v1i1.2889

Prayuda, R., & Sundari, R. (2018). Diplomasi dan *power*: Sebuah kajian analisis. *Journal of Diplomacy and International Studies*.

Rahman, L. L. A. (2020). Implikasi diplomasi pertahanan terhadap keamanan siber dalam konteks politik keamanan. *Jurnal Diplomasi Pertahanan, 6*(2), 2. https://doi.org/10.33172/jdp.v6i2.654

Rahmatika, A. N. (2022). Strategi pertahanan negara Indonesia dalam menghadapi ancaman artificial intelligence. *Jurnal Peperangan Asimetris, 8*(2). https://doi.org/10.33172/pa.v8i2.1511

Rosy, A. F. (2020, Juli). Indonesia's international cooperation: Strengthening national security in the field of cyber security. *Government Science (GovSci): Jurnal Ilmu Pemerintahan, 1*(2), 118–129. https://doi.org/10.54144/govsci.v1i2.12

Satori, D., & Sugiyono. (1992). *Metodologi penelitian kualitatif: Telaah positivistik rasionalistik, fenomenologik realisme metaphisik*. Rake Sarasin.

Sukandis, B. (2017). Peran diplomasi pertahanan Indonesia dalam kerjasama pertahanan Indonesia dan Amerika Serikat. *Jurnal Ilmu Hubungan Internasional, 1*(1), 12. https://doi.org/10.33822/jm.v1i1.285

Teong, Y. S. (2025, Februari). 19 juta serangan siber di Indonesia sepanjang 2024, ini kata pakar. *PROXSIS IT GRC*. https://it.proxsisgroup.com/19-juta-serangan-siber-di-indonesia-sepanjang-2024-ini-kata-pakar/

Wagiman, & Mandagi, A. S. (2016). *Terminologi hukum internasional*. Sinar Grafika.

Waskita, A. S., & Sidik, H. (2023, Agustus). Diplomasi siber Indonesia dalam penyelenggaraan capacity building on national cybersecurity strategy workshop 2019. *PADJIR, 5*(2), 122. https://doi.org/10.24198/padjir.v5i2.41337

Yin, R. K. (2018). *Case study research and applications: Design and methods*. SAGE Publications.