Konstitusi: Jurnal Hukum, Administrasi Publik, dan Ilmu Komunikasi
Volume. 2, Nomor. 3 Juli 2025
e-ISSN: 3063-4040; p-ISSN: 3063-3877, Hal 229-242
DOI: https://doi.org/10.62383/konstitusi.v2i3.852
*Available Online at:*https://ejournal.appihi.or.id/index.php/Konstitusi

Diplomasi Indonesia Menanggulangi ancaman digital

Eka Erlinda
Jurusan Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin, Indonesia

Alamat: Perintis Kemerdekaan No. KM. 10, Tamalanrea Indah, kec. Tamalanrea, Kota Makassar, Sulawesi Selatan 90245
*Korespondensi Penulis : erlindaeka355@gmail.com**

Abstract*. The development of digital technology has a major impact on the dynamics of national security, especially more complex cyber threats. The purpose of this study is to analyze Indonesian diplomacy in combating digital threats as part of efforts to strengthen non-military defense systems. The method used is a qualitative approach through literature research from various literary sources, reports, and secondary data. The results of the study show that while Indonesia is exposed to increasing cyber attacks, regulations on digital safety infrastructure and regulations are still weak compared to other ASEAN countries. The conclusion of this study is the importance of strategic and sustainable digital diplomacy, not just technically. The novelty of this study lies in cybersecurity threats as an analytical tool to assess the integration of digital diplomatic indicators, sensitivity to the system, and the effectiveness of Indonesian diplomacy in the growth of global cybersecurity.*

Keywords*: Cyber Security; Digital Diplomacy; Digital Threats; International Cooperation; National Resilience*

Abstrak. *Pengembangan teknologi digital memiliki dampak besar pada dinamika keamanan nasional, terutama ancaman cyber yang lebih kompleks. Tujuan dari penelitian ini adalah untuk menganalisis diplomasi Indonesia dalam memerangi ancaman digital sebagai bagian dari upaya untuk memperkuat sistem pertahanan non-militer. Metode yang digunakan adalah pendekatan kualitatif melalui penelitian literatur dari berbagai sumber sastra, laporan, dan data sekunder. Hasil penelitian menunjukkan bahwa sementara Indonesia terpapar pada peningkatan serangan siber, peraturan tentang infrastruktur dan peraturan keselamatan digital masih lemah dibandingkan dengan negara -negara ASEAN lainnya. Kesimpulan dari penelitian ini adalah pentingnya diplomasi digital strategis dan berkelanjutan, bukan hanya secara teknis. Kebaruan penelitian ini terletak pada ancaman keamanan siber sebagai alat analitik untuk menilai integrasi indikator diplomatik digital, sensitivitas terhadap sistem, dan efektivitas diplomasi Indonesia dalam pertumbuhan keamanan siber global.*

Kata kunci: : Ancaman Digital; Diplomasi Digital; Keamanan Siber; Kerja Sama Internasional; Ketahanan Nasional

1. LATAR BELAKANG

Pertumbuhan pesat teknologi mengacu pada perkembangan teknologi yang sangat cepat dan membawa perubahan besar dalam berbagai aspek kehidupan. Inovasi seperti kecerdasan buatan (AI), internet of things (IoT), jaringan 5G, dan komputasi awan telah mempermudah komunikasi, meningkatkan efisiensi kerja, serta mendorong kemajuan di bidang pendidikan, kesehatan, dan industri. Namun, kemajuan ini juga menimbulkan tantangan seperti ketimpangan digital, ancaman terhadap privasi, dan berkurangnya lapangan kerja akibat otomatisasi. Oleh karena itu, perkembangan teknologi perlu disertai dengan pemanfaatan yang bijak dan merata dimanahal ini telah menciptakan tantangan keamanan baru bagi pemerintah. Rendah Biaya Penerimaan, Anonimitas, Ketidakpastian di Wilayah Geografis, Dampak Dramatis dari, dan Kurangnya Transparansi Umum di Cyberspace telah menyebabkan

Received: Mei 17, 2025; Revised: Mei 31, 2025; Accepted: Juni 18, 2025; Online Available: Juni 20, 2025

kemunculan individu di mana pemerintah, organisasi dan kelompok teroris, dan bahkan individu di ruangan ini, termasuk ancaman yang mengancam para cybers Mayan Ini membedakan ancaman dari dunia maya, ancaman keamanan nasional tradisional. Ini sebagian besar transparan, dengan aktor adalah pemerintah dan negara, yang dapat diidentifikasi di wilayah geografis tertentu. Selama lebih dari tahun, analis telah mampu mencapai hasil dari serangan dunia maya(Li & Liu, 2021, p.1). Pertumbuhan pesat teknologi membuat masyarakat harus bergerak cerdas dalam menggunakan teknologi saat ini.

Di era digital saat ini, transformasi teknologi informasi menyebabkan perubahan besar dalam banyak aspek kehidupan, dari ekonomi dan politik hingga keamanan. Penggunaan teknologi memberikan peluang besar untuk efisiensi dan inovasi, tetapi juga membuka ruang untuk menumbuhkan ancaman cyber. Serangan siber sekarang bukan hanya individu, tetapi juga lembaga besar, perusahaan multinasional, dan pemerintah saja. Ini tidak hanya memiliki dampak ekonomi, tetapi juga mengarah pada hilangnya pada stabilitas sosial dan politik negara. Fenomena ini dapat dilihat dari peningkatan serangan cyber di berbagai daerah di dunia, Misalnya seperti Amerika Serikat, mengalami serangan pada jaringan Colonial Pipeline pada tahun 2021(Judianto, 2024, p.1). Indonesia pun tak luput dari ancaman ini.

Pada tahun 2016 hingga 2024 di Indonesia, kebocoran data meningkat secara signifikan, dengan sektor pemerintah menjadi target utama. Pada tahun 2024, peretasan Pusat Data Nasional Sementara menyebabkan gangguan yang luas, yang memengaruhi komunikasi pendidikan, imigrasi, dan lembaga. BSSN, badan keamanan siber Indonesia, juga menghadapi kerentanan, dengan situs Pusmanas-nya ditutup secara permanen pada tahun 2021 karena keterbatasan sumber daya manusia dan teknologi. Serangan ransomware Lockbit terhadap Bank Syariah Indonesia pada bulan Mei 2023 menyoroti konsekuensi ekonomi yang parah dari serangan siber, dengan data pelanggan bocor di darknet setelah negosiasi tebusan gagal. Penegak hukum berjuang untuk mengadili penjahat siber lintas batas, menggarisbawahi tantangan dalam menangani kejahatan siber internasional. Insiden ini menyoroti kebutuhan mendesak akan keamanan siber yang kuat untuk melindungi sistem pertahanan dan keamanan nasional, terutama dengan munculnya komputasi kuantum. Ancaman siber menimbulkan risiko terhadap otoritas pemerintah, integritas teritorial, dan reputasi TNI(Bhakti et al., 2024, p.113). Dunia maya memungkinkan terjadinya propaganda negatif, pencurian data, sabotase sistem, dan bahkan serangan pesawat nirawak. Oleh karena itu, menggabungkan teknologi canggih dengan sumber daya manusia yang terampil dan beretika sangat penting untuk mengurangi ancaman dunia maya di masa mendatang.

Ancaman digital yang bersifat bersifat lintas batas menjadi alasan pentingnya kerja sama internasional, Kerjasama internasional dalam pertahanan cyber menyediakan akses ke intelijen ancaman, teknologi, struktur kemampuan dan pertukaran praktik modern. Kerja sama ini tidak selalu membutuhkan pembentukan blok spesifik, tetapi membuka Path untuk berbagi informasi penting untuk tujuan intelijen. Secara regional, Indonesia telah secara aktif berpartisipasi dalam inisiatif keamanan siber sebagai anggota pendiri ASEAN. Dari 2017-2020 di, ASEAN telah mengembangkan strategi keamanan siber yang berfokus pada struktur kemampuan sertifikasi. Ini dikoordinasikan oleh pertemuan petugas digital ASEAN. Asean Digital Master Plan 2021 menyoroti pentingnya ruang digital sebagai pendorong utama pertumbuhan regional(Bhakti et al., 2024, p.116). Indonesia telah secara aktif berpartisipasi dalam inisiatif keamanan siber sebagai anggota pendiri ASEAN.

Diplomasi Indonesia dalam menangani dan mengatasi ancaman digital dilakukan melalui pendekatan bilateral, regional dan multilateral yang dikenal sebagai diplomasi dunia maya. Kementerian Luar Negeri, Siblis dan Otoritas Negara Bagian Sandy (BSSN) bekerja dengan Indonesia dengan berbagai negara, termasuk Australia dan AS, untuk meningkatkan kemampuan keamanan siber, termasuk pelatihan, pertukaran informasi dan pengembangan strategis nasional. Di tingkat regional, Indonesia aktif dalam bingkai ASEAN melalui strategi kerjasama keamanan siber ASEAN 2021-2025. Selain itu, Indonesia juga terlibat dalam dialog kebijakan dunia maya dengan negara -negara seperti Belanda untuk membahas kerangka kerja untuk kerja sama dalam keamanan siber, termasuk disinformasi dan peningkatan ketahanan digital. Global dibahas tentang norma dan prinsip perilaku tindakan nasional yang bertanggung jawab atas ruang maya. Melalui partisipasi ini, Indonesia telah berkontribusi pada pembentukan pemerintah dunia maya internasional yang aman dan damai. Diplomasi cyber ini membuat Indonesia ingin memperkuat ketahanan digital negara dan memainkan peran aktif dalam menciptakan ekosistem cyber global yang aman dan andal(Saputri, Surryanto D. W. and Helda Risman, 2020). Diplomasi Indonesia untuk mengatasi ancaman digital akan dilakukan melalui kerja sama regional, termasuk pelatihan cyber dengan ASEAN dan Jepang. Fokusnya adalah untuk meningkatkan kemampuan teknis staf yang menghadapi serangan siber. Namun, tantangannya adalah bahwa diplomasi ini tetap terbatas pada aspek teknis, tidak membahas pedoman strategis dan bergantung pada dukungan negara -negara mitra.

2. KAJIAN TEORITIS

Diplomasi Indonesia

Diplomasi merupakan hal yang banyak mengubah dunia dalam perkembangannya. Dimulai dari berbagai upaya untuk sampai kepada NKRI hingga akhirnya mencapai titik diplomasi digital, yang mana kita ketahui kalau semua yang berhubungan dengan digital akan berkembang pesat disetiap zamannya. Semua upaya untuk diplomasi Indonesia kenegara lain telah diupayakan, mulai dari mengikuti trend zaman sekarang hingga penelitian apa yang sedang digandrungi akhir akhir ini (Nur, 2023). Adapun bentuk bentuk diplomasi iyalah sebagai berikut.

1. Diplomasi publik

   Hans Tuch mendefinisikan Diplomasi publik adalah sebagai bentuk proses komunikasi pemerintah negara -negara dengan pemangku kepentingan asing yang mencoba menjelaskan ide dan cita -cita Semua negara, lembaga, budaya, dan kepentingan dan pedoman nasional. Tujuan dan manfaat warga diungkapkan oleh orang asing ada banyak pilihan, termasuk program internasional, jurnalis pelatihan dan akademisi. orang asing, organisasi budaya dan pertukaran, kunjungan, rapat yang direncanakan; penerbitan (Nur, 2023). Diplomasi merupakan suatu bentuk strategi suatu negara dalam melakukan berbagai keperluan yang menyangkut urusan kenegaraan.

2. Diplomasi Digital

   Diplomasi digital digunakan sebagai cara baru diplomasi internet dan teknologi digital juga merupakan penggunaan Internet dan penggunaan Internet. Teknologi informasi dan komunikasi baru untuk mencapai tujuan diplomatik. Diplomasi digital ini juga merupakan pengembangan diplomasi publik dan dilakukan oleh negara. Penggunaan perangkat teknologi digital seperti internet dan media sosial (Nur, 2023). Dengan adanya digital diplomasi bisa dikatakan ini adalah peluang besar bagi berbagai negara negara untuk memanfaatkannya.

Diplomasi publik Indonesia adalah upaya pemerintah untuk membangun citra positif negara di mata dunia dengan menggunakan kekuatan budaya, nilai -nilai politik, dan komunikasi persuasif. Pendekatan ini adalah bagian dari kekuatan lunak dan harus memiliki efek yang damai dan sukarela. Diplomasi digital lahir sebagai penggunaan internet dan media sosial, yaitu penggunaan internet dan media sosial, untuk mendukung tujuan diplomasi publik. Diplomasi digital memungkinkan pesan pemerintah Indonesia diteruskan lebih cepat, umumnya dan ke komunitas internasional interaktif. Kedua bentuk diplomasi adalah strategi utama untuk Indonesia dan memperkuat globalisasi dan posisinya saat ini di tengah kompetisi nasional (Surya, 2023). Diplomasi publik dan diplomasi digital merupakan salah satu strategi negara Indonesia dalam mengejar ketertinggalan globalisasi.

Gambar 1. Indicators of The Indonesian Diplomacy

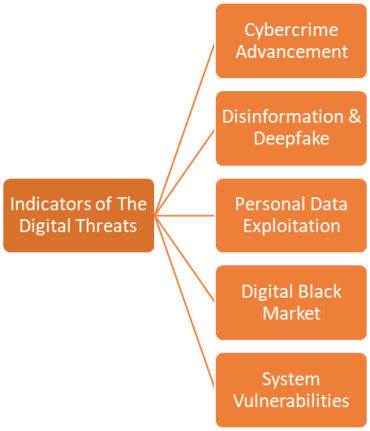
Ancaman digital

Pengembangan teknologi digital seperti data besar, Internet of Things (IoT), kecerdasan buatan (AI), pembelajaran mesin, dan cryptocurrency memiliki dampak besar pada kehidupan modern, tetapi ada juga berbagai ancaman baru di dunia maya. Cybercrime terus mencari kesenjangan dalam menggunakan kemajuan teknologi untuk keuntungan pribadi, seperti mengotomatiskan serangan dan menyediakan layanan kejahatan sebagai layanan. AI adalah alat utama untuk banyak ancaman digital modern. Dalam crypto -asset -ökosystem, AI untuk penipuan digunakan untuk menyebarkan disinformasi besar melalui produksi paus dalam, manipulasi pasar dengan token palsu. Model suara skala besar (LLM) juga digunakan oleh peretas dan aktor negara untuk mengenali kesenjangan keamanan dan eksploitasi desain. Selain itu, AI mendukung penciptaan pasar gelap digital. Digital Black Market secara terbuka menjual layanan seperti membuat dokumen palsu dan membuat konten pur yang eksplisit. Salah satu bentuk serangan yang paling umum adalah phishing berbasis AI. Phishing ini menggunakan model suara seperti chatgpt untuk membuat email cross-linguistik, persuasif, dan penipuan dan terjemahan yang memungkinkan kolaborasi antara kelompok kriminal dengan persimpangan. Penjahat juga akan menggunakan teknologi audio dan video Deeppake untuk mengambil langkah -langkah tertentu, termasuk penyamaran untuk memeriksa identitas digital yang digunakan di bank dan platform kriptografi, untuk menipu para korban (Konferensi, 2024). Ancaman digital saat ini cukup banyak jenisnya dan sebagai warga negara harus bisa menggunakan beberapa jenis seperti AI dengan cerdas.

Ancaman lain adalah munculnya layanan "jailbreak", yang memungkinkan pengguna untuk menyusup ke pembatasan penggembalaan untuk membuat konten berbahaya seperti malware dan instruksi phishing. Penyerang menggunakan kesenjangan sistem dalam berbagai cara. B. Pertanyaan hipotetis atau bahasa asing untuk menghindari pengakuan. AI juga

digunakan untuk melakukan atau mengungkapkan identitas pribadi secara online. Model bahasa skala besar dilatih dari sejumlah besar data publik, memungkinkan mereka untuk mengumpulkan informasi pribadi seperti lokasi, pekerjaan, dan etnis. Semakin banyak data pribadi didistribusikan melalui internet, semakin tinggi risiko bagi pengguna. Produktivitas pelaku meningkat dengan cepat bersama dengan alat-alat seperti cacing berbasis basis cacing, yang dapat diubah karena kejahatan. Penyakit ini juga menunjukkan bahwa ia juga memiliki tantangan keamanan yang semakin kompleks di sepanjang jalan, menunjukkan kewaspadaan yang tinggi dari semua pihak yang terlibat (Konferensi, 2024). Dalam menggunakan internet harus sangat berhati hati mengingat Semakin banyak data pribadi didistribusikan melalui internet, semakin tinggi risiko bagi pengguna.

Revolusi digital tidak hanya opsional, tetapi merupakan suatu keharusan bagi setiap negara untuk memastikan pertumbuhan ekonomi. Indonesia adalah negara berkembang dengan populasi besar dan potensi ekonomi yang besar. Konversi digital merupakan bagian dari salah satu pilar utama untuk mencapai istilah visi pengembangan jangka panjang. Namun demikian, perjalanan ke transformasi digital tidak dapat dipisahkan dari kompleksitas ancaman yang muncul di dunia digital yang dinamis. Indonesia telah mengidentifikasi transformasi pada waktu yang didominasi oleh kemajuan teknologi digital Digital sebagai pendorong utama untuk mencapai dan meningkatkan pertumbuhan ekonomi yang berkelanjutan daya saing nasional. Transformasi digital menawarkan banyak peluang untuk kemajuan, tetapi tidak, tidak kita dapat menyangkal bahwa dunia digital menimbulkan ancaman dan risiko yang membutuhkan perhatian. Bersedia menghadapi dunia digital untuk mempercepat transformasi digital Indonesia mencerminkan kebutuhan mendesak dengan tujuan memahami dan mengatasi kemungkinan risiko dibuat selama perjalanan transformasi digital di Indonesia (Journal *et al.*, 2024). Indonesia telah mengidentifikasi transformasi pada waktu yang didominasi oleh kemajuan teknologi digital Digital sebagai pendorong utama untuk mencapai dan meningkatkan pertumbuhan ekonomi yang berkelanjutan daya saing nasional.



Gambar 2. Indicators of the Digital Threats

3. METODE PENELITIAN

Studi ini dilakukan dengan menggunakan pendekatan kualitatif untuk menyelidiki dan menganalisis dampak keamanan pada pengembangan pariwisata maritim di Indonesia. Berdasarkan definisi itu, penelitian kualitatif digunakan untuk memahami bagaimana seseorang melihat lingkungannya. Ada banyak pendekatan untuk penelitian kualitatif, tetapi setiap orang cenderung beradaptasi dengan makna agresif ketika menafsirkan dan memfokuskannya. Tujuan dari penelitian kualitatif adalah untuk mencapai pemahaman komprehensif tentang fenomena sosial, termasuk kualitas fenomena di lingkungan alam(Ugwu, Chinyere, N; Eze Val, 2017). Data Peneliti menggunakan sumber data berupa literature review (artikel, jurnal, berita, website). Selama penelitian peneliti melakukan proses analisis mengenai pengaruh keamanan terhadap perkembangan pariwisata maritim di Indonesia dengan menggunakan sumber data tersebut.

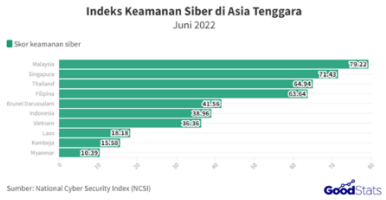
4. HASIL DAN PEMBAHASAN

Gambar 3. Jumlah Serangan Tahun 2021 di Indonesia

Sumber: https://www.researchgate.net/figure/Gambar-2-Jumlah-Serangan-Tahun-2021-di-Indonesia-Badan-Sandi-dan-Siber-Negara-2022_fig2_376382053 (‘Gambar-2-Jumlah-Serangan-Tahun-2021-di-Indonesia-Badan-Sandi-dan-Siber-Negara-2022’, no date).

Pada gambar 3 menunjukkan perkembangan jumlah serangan yang terjadi setiap bulan sepanjang tahun 2021. Secara umum, terdapat tren peningkatan jumlah serangan dari awal hingga akhir tahun. Pada bulan Januari, jumlah serangan dicatat di 59.316.206, tetapi pada bulan Februari turun menjadi 44.901.308. Kemudian tren dengan 186.202.637 serangan dari Maret, dari klimaks pertama Maret hingga Mei. Kenaikan ini berlanjut pada bulan Juni yang mencatat angka lebih tinggi, yaitu 244.446.175. Namun, pada bulan Juli hingga September, jumlah serangan mengalami penurunan bertahap, mencapai titik terendah di bulan September sebesar 123.695.909. Kemudian meningkat secara signifikan dari Oktober hingga Desember, dengan jumlah serangan tertinggi di 242.066.168 pada bulan Desember. Pola ini menunjukkan peningkatan yang signifikan dalam aktivitas serangan di menengah dan tahun. Ini bisa menjadi masalah khusus dalam upaya untuk memperkuat sistem keamanan, terutama pada akhir tahun. Pada kondisi ini indicator yang paling berkaitan adalah Digital Engagement.

Indikator Digital Engagement adalah salah satu indikator yang paling relevan dalam konteks diplomasi Indonesia. Di zaman globalisasi dan revolusi digital, partisipasi melalui platform digital adalah kunci untuk menyampaikan pesan diplomatik dengan cepat, cepat dan efektif ke komunitas internasional. Pemerintah Indonesia semakin banyak menggunakan media sosial, lokasi resmi dan berbagai saluran digital untuk memperkenalkan budaya dan membangun dua cara untuk mengkomunikasikan posisi dan pedoman asing secara transparan. Strategi ini tidak hanya memperluas ruang lingkup diplomasi, tetapi juga memungkinkan mata global untuk mempercayai dan memperkuat citra Indonesia. Selain itu, komitmen digital Indonesia memungkinkan kita untuk tetap dalam keadaan darurat seperti pandemi dengan mitra internasional, memberikan cara penting untuk mencapai generasi muda global yang lebih agresif di ruang digital.



Gambar 4. Indeks keamanan Siber di Asia Tenggara

Sumber: https://goodstats.id/article/indeks-keamanan-siber-indonesia-jauh-lebih-buruk-dari-malaysia-ini-grafiknya-GQkGl ('NCSI JUNI 2022', no date)

Pada gambar 4 menjelaskan dan menunjukkan nilai peringkat dan keamanan negara - negara di wilayah Asia Tenggara berdasarkan data dari National Cyber Security Index (NCSI). Dalam grafik, Malaysia mencetak posisi terbaik dengan skor 79,22, dengan Singapura mencetak skor 71,43 dan skor 64,94 di Thailand. Ketiga negara ini menunjukkan tingkat

motivasi dan perlindungan dunia maya yang tinggi dibandingkan dengan negara lain di wilayah tersebut. Filipina diikuti dengan skor 63,64 di keempat, diikuti oleh Brunei Dalsalam (41,56) dan Indonesia (38,96). Skor Indonesia diklasifikasikan sebagai pertengahan hingga rendah. Ini menunjukkan bahwa sistem keamanan siber nasional perlu ditingkatkan. Negara -negara seperti Vietnam (36.36), Laos (18.18), Kamboja (15.58) dan Myanmar (10.39) menunjukkan kurangnya kemauan untuk menangani ancaman dunia maya. Data ini menunjukkan bahwa Indonesia dan beberapa negara Asia Tenggara lainnya masih menghadapi tantangan besar dalam memperkuat sistem keamanan digital mereka ketika mereka semakin bergantung pada teknologi informasi dan komunikasi. Pada kondisi ini indicator yang relevan adalah System Vulnerabilities.

Indikator System Vulnerabilities sangat relevan dalam konteks kondisi keamanan siber Indonesia karena mencerminkan akar dari berbagai permasalahan yang menyebabkan rendahnya skor keamanan digital. Kerentanan sistem mengacu pada kelemahan dalam infrastruktur teknologi informasi, baik dari sisi perangkat keras, perangkat lunak, maupun prosedur operasional, yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan serangan. Dalam kasus Indonesia, skor 38,96 dalam indeks keamanan siber menunjukkan bahwa masih terdapat banyak celah dalam sistem yang belum terlindungi secara optimal, seperti kurangnya firewall yang kuat, lemahnya enkripsi data, serta lambatnya pembaruan sistem keamanan. Selain itu, rendahnya kesadaran keamanan digital di kalangan institusi dan masyarakat, serta keterbatasan tenaga ahli di bidang siber, memperbesar risiko kebocoran data dan serangan digital.

Dengan berkembangnya peran teknologi digital dalam diplomasi masa kini, tantangan keamanan siber pun semakin meningkat. Ketergantungan pada platform digital untuk interaksi dan negosiasi menjadikan lembaga diplomatik mudah diserang siber, dibobol, dan mengalami kebocoran data. Peristiwa seperti peretasan email DNC pada 2016 memperlihatkan bagaimana elemen siber dapat memengaruhi pemilihan umum dan hubungan global. Spionase siber dan pencurian informasi rahasia pemerintah kini menjadi tantangan besar, ditambah dengan banyaknya disinformasi dan penyebaran konten palsu seperti deepfake yang mengganggu kredibilitas diplomatik. Dalam mengatasi hal tersebut, banyak negara mengalokasikan dana untuk strategi keamanan siber dan meningkatkan ketahanan digital. Akan tetapi, kompleksitas serangan siber semakin meningkat, memerlukan pendekatan yang lebih menyeluruh, seperti penerapan protokol keamanan, pelatihan bagi diplomat, dan kolaborasi internasional. Dalam situasi ini, keamanan siber menjadi faktor penting dalam mempertahankan stabilitas dan integritas diplomasi internasional (Yousaf, 2024). Keamanan siber perlu perhatian tinggi

dengan tetap menggunakan platform digital dengan cerdas dan pada kondisi ini indicator yang relevan adalah Cybersecurity Threats.

Indikator Cybersecurity Threats sangat terkait karena secara langsung menunjukkan tantangan signifikan yang dihadapi oleh diplomasi digital saat ini. Perlu diketahui sebelumnya, disebutkan bahwa pelaksanaan diplomasi semakin tergantung pada teknologi digital, tetapi ketergantungan itu juga menciptakan peluang untuk berbagai jenis serangan siber seperti hacking, kebocoran informasi, spionase digital, dan kampanye disinformasi. Ancaman-ancaman ini tidak hanya mengganggu fungsi lembaga diplomatik, tetapi juga dapat berdampak pada pemilu, merusak hubungan antar negara, dan mengancam keamanan nasional. Di samping itu, hadirnya teknologi manipulatif seperti deepfake memperparah penyebaran informasi tidak benar yang bisa mengganggu proses negosiasi serta kepercayaan diplomatik.

Keterhubungan yang kuat antara internet dan diplomasi telah meningkatkan pentingnya diplomasi digital, termasuk di Indonesia. Pelaksanaan diplomasi telah memungkinkan kebijakan luar negeri dapat diakses oleh masyarakat melalui berbagai alat teknologi informasi dan komunikasi. Kementerian luar negeri, kedutaan, dan duta besar (termasuk para diplomat) menunjukkan minat yang semakin besar untuk membagikan kegiatan diplomatik mereka kepada publik. Kementerian Luar Negeri Indonesia telah melaksanakan beragam kebijakan untuk menangani isu diplomasi digital. Alih-alih hanya memberikan informasi kepada masyarakat melalui berbagai akun media sosial, kesiapan Kementerian Luar Negeri secara signifikan mencerminkan kebijakan pemerintah untuk membuat negara lebih hadir bagi masyarakat Indonesia, baik di dalam negeri maupun di kancah internasional di era digital saat ini. Dengan adanya DCC untuk mendukung kegiatan diplomasi digitalnya, Kementerian Luar Negeri Indonesia perlu bekerja keras untuk membangun kerjasama dengan kementerian lainnya dengan fokus khusus pada pencarian strategi dalam menghadapi peningkatan kegiatan siber termasuk serangan siber. Pemerintah Indonesia memerlukan kebijakan tambahan untuk merumuskan strategi nasional bagi diplomasi digital guna menangani peningkatan penggunaan media sosial sebagai sarana interaksi antar masyarakat dari berbagai negara (Madu, 2018). Diplomasi telah meningkatkan pentingnya diplomasi digital termasuk di Indonesia, pada kondisi ini indicator yang relevan adalah Digital Diplomacy Readiness.

Indikator Digital Diplomacy Readiness penting karena menunjukkan usaha suatu negara dalam menggunakan teknologi digital untuk memperkuat komunikasi dan pelaksanaan kebijakan luar negeri. Dalam hal ini, kemampuan lembaga diplomatik dalam memanfaatkan media sosial, menjalin hubungan antar kementerian, dan merumuskan strategi untuk menghadapi tantangan di dunia digital menjadi sangat krusial. Kehadiran suatu negara di dunia

digital bukan sekadar untuk menyampaikan informasi, tetapi juga berkenaan dengan kemampuan untuk beradaptasi terhadap perubahan cepat dan rumit dalam komunikasi global. Di samping itu, kesadaran akan perlunya strategi nasional dan kerja sama antar lembaga mencerminkan adanya proses transisi menuju diplomasi yang lebih terbuka, responsif, dan berbasis teknologi. Seluruh elemen ini mengindikasikan bahwa kesiapan dalam diplomasi digital adalah indikator penting untuk menilai seberapa jauh suatu negara dapat menggabungkan teknologi ke dalam praktik hubungan internasionalnya.

Pada 2017, pemerintah Indonesia menunjukkan keseriusan dalam menangani ancaman dunia maya melalui pembentukan lembaga -lembaga khusus, yaitu pembentukan Siwa dan Institusi Sandi (BSSN) di negara bagian tersebut. BSSN telah diminta untuk mengembangkan pedoman teknis dan operasional di bidang keamanan siber dan menjadi pusat koordinasi insiden digital. Sebelum yayasan BSSN, Indonesia memiliki ID-SIRTII (tim respons insiden keamanan Indonesia di infrastruktur internet) sebagai tim respons insiden, bekerja dengan berbagai partai politik seperti APJII, Polri, Masti. Inisiatif ini menunjukkan pemahaman Indonesia tentang pentingnya terapi cyber sistematis. Infrastruktur terbatas, seperti kurangnya satelit independen dan kurangnya pendidikan publik, merupakan tantangan besar dalam implementasi (Mahendra and Pinatih, 2023). BSSN adalah salah satu bentuk Upaya Indonesia dalam menanggulangi ancaman digital.

Selain menciptakan sebuah lembaga, Indonesia juga telah menerbitkan banyak pedoman hukum seperti ITE Law No. 11/2008 dan PP No. 82/2012, tetapi sejauh ini tidak ada undang -undang khusus yang secara komprehensif mengatur keamanan siber. Kurangnya peraturan yang kuat adalah penghalang untuk respons terhadap ancaman digital yang lebih kompleks dan komprehensif. Faktanya, Security and Resilience (KKS) Shiver Act, yang diharapkan didasarkan pada hukum nasional, dibatalkan pada 2019. Sementara itu, kemampuan keamanan digital populasi Indonesia masih rendah, dan jumlah pakar cybersecurity bersertifikat minimal. Oleh karena itu, strategi untuk menangani keamanan siber di Indonesia tetap menjadi tantangan utama dalam hal legalitas, SDM dan pengembangan infrastruktur digital belaka (Mahendra and Pinatih, 2023). Upaya atau kemampuan Indonesia dalam menanggulangi ancaman digital terbilang lemah.

Cybersecurity di Indonesia adalah ekosistem yang kompleks yang mencakup aspek hukum, kelembagaan, keterampilan teknis, kolaborasi lintas sektor dan pengembangan teknologi berkelanjutan. Dalam implementasinya, tantangan ini muncul dari koordinasi pemangku kepentingan, kemampuan keamanan digital yang rendah, dan kurangnya koordinasi antara peraturan yang optimal dan infrastruktur organisasi. Sosialisasi kompetensi dan standar

pendidikan publik tidak terdistribusi secara merata, terutama di antara kelompok usia yang lebih muda, pengguna internet terbesar. Istilah hukum, peraturan yang ada tidak menanggapi sepenuhnya dinamika cyber, tetapi ratifikasi peraturan baru, seperti RUU data pribadi, dianggap mendesak. Dari sisi organisasi, transformasi kelembagaan tunduk pada pembatasan birokrasi seperti kombinasi fungsi dan BSSN. Sementara itu, kerja sama internasional diikuti oleh lembaga-lembaga seperti ID Certs dan ID-Sirtii, tetapi sifatnya yang terbatas dan efektivitas sukarela mereka terpengaruh. Pengembangan teknologi seperti IoT dan Cloud Computing juga menimbulkan tantangan teknis yang memperluas kesenjangan dalam serangan cyber. Oleh karena itu, memperkuat sistem keamanan digital nasional membutuhkan pendekatan komprehensif yang berfokus tidak hanya pada teknologi, tetapi juga pada reformasi kelembagaan, regulasi, pendidikan, dan kerja sama global terstruktur (Mahendra and Pinatih, 2023). Indonesia masih memiliki beberapa tantang dalam menangani ancaman digital.

Sementara kondisi keamanan siber Indonesia saat ini menunjukkan kemajuan struktural, mereka masih dibayangi oleh tantangan utama yang terkait dengan peraturan, koordinasi lintas sektor dan persiapan SDM. Lembaga -lembaga seperti BSSN dibentuk dan berbagai pedoman dasar diimplementasikan, seperti UU ITE dan undang -undang yang melindungi data pribadi, tetapi implementasi tidak optimal. Sebuah studi oleh Dewi & Suryandari (2022) menyoroti bahwa kelemahan besar yang tidak terisi dari kerangka politik yang terputus -putus, kurangnya pendidikan publik dan kurangnya para ahli keamanan siber yang terakreditasi berbohong. Selain itu, kerja sama dengan sektor swasta dalam pengembangan sistem keamanan digital tetap menantang dalam hal kepercayaan dan informasi terbuka. Dalam konteks ini, Indonesia harus memperkuat tata kelola keamanan siber dengan sektor lintas sektor dan dukungan politik yang lebih luas (Dewi & Suryandari, 2022). Indonesia masih menghadapi tantangan keamanan siber akibat lemahnya koordinasi, minimnya SDM ahli, dan belum optimalnya regulasi.

KESIMPULAN

Cybersecurity saat ini merupakan pilar penting dari sistem pertahanan non-militer Indonesia, terutama di tengah mempercepat transformasi digital global. Kemajuan teknologi seperti AI, IoT, dan komputasi awan tidak hanya memberikan peluang untuk kemajuan, tetapi juga menimbulkan risiko serius dalam bentuk serangan cyber-batas, pencurian data, disinformasi dan manipulasi politik. Indonesia adalah B. Mereka terpapar berbagai insiden penting, termasuk serangan ransomware pada Pusat Data Nasional dan sektor keuangan. Sayangnya, infrastruktur yang lemah, kurangnya sumber daya manual dan peraturan untuk para

profesional masih suboptimal. Sistem Keamanan NasionalCy tetap rentan. Ini adalah ancaman terhadap kedaulatan digital, integritas nasional dan reputasi internasional.

Menanggapi tantangan ini, Indonesia telah mengembangkan diplomasi digital sebagai strategi penting. Indonesia akan berupaya meningkatkan ketahanan digital melalui pelatihan, pertukaran informasi dan dialog politik, terutama melalui kerja sama bilateral dan multilateral dalam kerangka ASEAN, dan dengan mitra seperti AS dan Australia. Namun, strategi ini tetap teknis dan tidak menyentuh aspek strategis jangka panjang. Ini membutuhkan pendekatan yang lebih komprehensif, termasuk reformasi peraturan, peningkatan literasi digital di depan umum, peningkatan regulasi silang, dan pengembangan co-ekosistem antara pemerintah, sektor swasta dan masyarakat. Persiapan yang matang dari diplomasi digital memungkinkan Indonesia memainkan peran yang lebih kuat dalam menciptakan ruang maya yang aman, terintegrasi, dan berkelanjutan.

DAFTAR REFERENSI

Badan Sandi dan Siber Negara. (2022). Jumlah serangan tahun 2021 di Indonesia. [Gambar]. https://bssn.go.id (gunakan ini jika nama sumber jelas; jika tidak, gunakan judul sebagai entri pertama)

Bhakti, A., et al. (2024). State defense strategy in facing cyber threats after hacking incidents on government institutions: A case study in Indonesia. Jurnal Ilmiah, 20(1), 109–117.

Dewi, A. R., & Suryandari, D. (2022). Penerapan strategi keamanan siber nasional di Indonesia: Analisis regulasi dan implementasi. Jurnal Ilmiah Kebijakan Publik, 8(1), 15–26.

IDOSR. (2017). International Digital Organization for Scientific Research (IDOSR). Idosr Journal of Science and Technology, 3(1), 37–46. http://www.idosr.org

Journal, I., et al. (2024). Digital world threat preparedness for digital transformation acceleration policy in Indonesia. Journal Ilmiah, 4(1), 140–150.

Judianto, L. (2024). National security strategies amidst increasing global cyber threats: A multilateral approach. Journal of Security Studies, 1(November), 11–18.

Konferensi, M. (2024). SVISHTOV - Cabang Svishtov Konferensi ilmiah internasional. https://doi.org/10.58861/tae.pcesetfc.2024.39

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. Energy Reports, 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Madu, L. (2018). Indonesia's digital diplomacy: Problems and challenges. Jurnal Hubungan Internasional, 7(1). https://doi.org/10.18196/hi.71121

Mahendra, Y. C., & Pinatih, N. K. D. S. A. (2023). Strategi penanganan keamanan siber (Cyber Security) di Indonesia. Jurnal Review Pendidikan dan Pengajaran (JRPP), 6(4), 1941–1949. http://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/20659

NCSI. (2022, Juni). NCSI 2022. [Data tidak dipublikasikan secara lengkap – sesuaikan jika ada sumber resmi]

Nur, S. (2023). Pengantar diplomasi: Ujian akhir semester. [Materi tidak dipublikasikan].

Saputri, D. P., Surryanto, D. W., & Risman, H. (2020). The Indonesian cyber diplomacy: ASEAN-Japan online cyber exercise. Technium Social Sciences Journal, 9, 453–464. https://doi.org/10.47577/tssj.v9i1.911

Surya, I. A. (2023). The history of Indonesian diplomacy, public diplomacy, and digital diplomacy of the Indonesian government. ResearchGate. https://www.researchgate.net/publication/367190601

Yousaf, M. (2024). The evolution of diplomacy in the digital age: Opportunities and challenges. ResearchGate. https://doi.org/10.13140/RG.2.2.16396.42889