ICODEV: Indonesian Community Development Journal
Vol. 6, No. 1, Januari 2025, 39-52
ISSN: 2775-1538 (online)

Peran Diplomasi Siber Indonesia dalam Melindungi Keamanan Teknologi E-Commerce Nasional

Fany Anggun Abadi[1], Rifqi Itsnaini Yusuf[2], Intan Tiara Kartika[3]*
[1,2]Universitas Peradaban, Brebes, Indonesia
[3]Universitas Negeri Gorontalo, Gorontalo, Indonesia

Article Information
Submitted March 05, 2025
Revision April 01, 2025
Accepted April 22, 2025
Published May 20, 2025

Abstract

This article examines Indonesia's cyber diplomacy efforts in safeguarding national e-commerce technology security amidst the challenges posed by cross-border cyber threats. Employing a qualitative methodology and the actor-network theory approach, this study highlights the urgency of cyber diplomacy as a strategic instrument to address vulnerabilities in the e-commerce sector against cyberattacks. The rapid growth of Indonesia's digital economy has been accompanied by increasing threats such as data breaches, malware attacks, and disinformation campaigns, necessitating multistakeholder collaboration and robust regulatory frameworks. This paper underscores the importance of a multidisciplinary approach and international cooperation through cyber diplomacy to enhance national cybersecurity. Cyber diplomacy encompasses not only technical dimensions but also the development of international norms, data protection, and the enhancement of human resource capacity. The study further identifies critical challenges, including low levels of digital literacy among the population and regulatory unpreparedness, and offers recommendations to strengthen bilateral and multilateral cooperation.

Keywords: Cyber diplomacy, Cybersecurity, E-commerce, Digital Threats, International collaboration.

Tulisan ini mengkaji peran diplomasi siber Indonesia dalam melindungi keamanan teknologi e-commerce nasional di tengah tantangan ancaman siber lintas batas. Dengan menggunakan metode kualitatif dan pendekatan teori jaringan aktor, penelitian ini menyoroti urgensi diplomasi siber sebagai instrumen strategis untuk mengatasi kerentanan sektor terhadap serangan siber. Pesatnya pertumbuhan ekonomi digital di Indonesia diiringi oleh peningkatan ancaman seperti pencurian data, serangan e-commerce malware, dan disinformasi, yang menuntut kolaborasi multistakeholder dan kerangka regulasi yang kuat. Artikel ini menekankan pentingnya pendekatan multidisipliner dan kerjasama internasional melalui diplomasi siber untuk memperkuat keamanan siber nasional. Diplomasi siber tidak hanya mencakup aspek teknis, tetapi juga pembentukan norma internasional, perlindungan data, dan peningkatan kapasitas sumber daya manusia. Studi ini juga mengidentifikasi tantangan seperti rendahnya literasi digital masyarakat dan ketidaksiapan regulasi, serta menawarkan rekomendasi untuk memperkuat kerjasama bilateral dan multilateral

Kata Kunci: diplomasi siber, keamanan siber, e-commerce, ancaman digital, kolaborasi internasional

***Author Correspondence**: Fany Anggun Abadi, anggunabadi1998@gmail.com, Brebes, Jawa Tengah, Indonesia, 52274

Copyright © 2025 Fany Anggun Abadi, Rifqi Itsnaini Yusuf, Intan Tiara Kartika

Pendahuluan

Kemajuan teknologi telah berkembang pesat seiring dengan berbagai inisiatif global, seperti Revolusi Industri 4.0 yang telah dikenal secara luas. Pertumbuhan ekonomi lokal yang berkelanjutan dan peningkatan kesejahteraan pelaku Usaha Mikro Kecil dan Menengah (UMKM) telah menjadi fokus utama bagi berbagai kebijakan pemerintah di berbagai wilayah (Amaria, K. H & Ulinnuha, Roma,, 2023) Perkembangan ini mencakup pemanfaatan internet, teknologi komputasi awan, kecerdasan buatan, robotika, serta berbagai inovasi digital lainnya yang dirancang untuk mendukung aktivitas manusia. Meski membawa sejumlah manfaat, transformasi teknologi ini juga memberikan implikasi signifikan terhadap dinamika politik, baik di tingkat nasional maupun internasional. Seiring berjalannya waktu, sejumlah perubahan struktural dan kebijakan telah muncul sebagai respons terhadap perkembangan teknologi tersebut. (Edition, F. D. 2013).

Interaksi masyarakat digital dalam memanfaatkan internet sangat dipengaruhi oleh aspek ketersediaan, integritas, dan kerahasiaan informasi di ranah siber. Di tingkat global, negara-negara serta komunitas internasional perlu merumuskan strategi kolaboratif guna merespons dinamika perkembangan dunia maya yang bersifat lintas batas. Salah satu upaya yang dapat dilakukan adalah dengan merumuskan norma-norma internasional yang mengatur berbagai isu dan potensi ancaman di ruang siber. (Chotimah, H. C. 2019).

Pada tingkat nasional, kemajuan teknologi telah memberikan dampak signifikan terhadap birokrasi, terutama dengan mendorong partisipasi publik yang lebih luas. Hal ini turut memengaruhi proses formulasi kebijakan dan pengambilan keputusan pemerintah, baik dalam bentuk dampak positif maupun tantangan baru (Edition, F. D., 2013). Sementara itu, pada tataran internasional, perkembangan teknologi telah melahirkan bentuk-bentuk konflik kontemporer. Jika dahulu konflik bersifat konvensional dengan penggunaan senjata api, bom, dan kendaraan tempur, kini konflik dapat terjadi di ranah digital, misalnya melalui aksi pencurian data atau informasi oleh aktor negara lain. (Edition, F. D. 2013).

Dalam bukunya, Barston (2014) menyatakan bahwa kemajuan teknologi telah menyebabkan empat transformasi mendasar dalam praktik diplomasi kontemporer. Pertama, teknologi mengubah dinamika ruang dan waktu dalam interaksi diplomatik. Kedua, arus informasi yang melimpah melalui media massa menyulitkan penerapan pendekatan diplomasi tradisional dalam menilai isu atau mengelola konflik. Ketiga, batas antara ranah privat dan publik menjadi semakin kabur akibat perkembangan teknologi informasi. Keempat, revolusi teknologi menciptakan potensi ancaman baru terhadap sistem diplomasi yang telah mapan. Oleh karena itu, Barston menegaskan pentingnya pendekatan diplomasi siber dalam menghadapi tantangan-tantangan tersebut. (Barston, 2014).

Seiring dengan meningkatnya isu keamanan siber di tingkat global, Indonesia dinilai masih kurang proaktif dalam keterlibatannya di bidang tersebut. Hingga saat ini, Indonesia belum menjalin kesepakatan bilateral maupun multilateral terkait regulasi dan kerjasama di sektor siber, meskipun ancaman terhadap keamanan sibernya terus meningkat. Data pada tahun 2018 mencatat bahwa Indonesia mengalami lebih dari 200

juta serangan siber (Valentina, 2019). Selain itu, perusahaan keamanan digital Kaspersky memperkirakan bahwa Indonesia akan menghadapi potensi serangan siber selama penyelenggaraan Pemilihan Presiden 2019, khususnya yang berkaitan dengan upaya pemalsuan data suara. (Nityasari, A. 2020).

Seiring dengan meningkatnya isu keamanan siber di tingkat global, perhatian Indonesia terhadap perlindungan di ranah digital mulai tampak sejak tahun 2007, yang ditandai dengan diterbitkannya undang-undang pertama yang mengatur protokol internet guna menjamin keamanan sistem telekomunikasi nasional. (Ardipandanto, A., & Budiman, A. 2018).

Indonesia pernah mengalami tantangan serius dalam keamanan siber, seperti yang tercatat pada tahun 2018 ketika terjadi lebih dari 200 juta serangan siber (Valentina, 2019). Menurut prediksi Kaspersky, potensi serangan siber juga mengancam proses Pemilihan Presiden 2019, khususnya terkait kemungkinan pemalsuan data suara. Prediksi tersebut didasarkan pada kejadian sebelumnya, di mana proses pengumpulan data untuk keperluan hitung cepat mengalami gangguan (Nityasari, 2020). Pelaku serangan siber tidak hanya berasal dari luar negeri, tetapi juga dapat merupakan warga Indonesia sendiri. Di sisi lain, identifikasi pelaku melalui alamat Internet Protocol (IP) memiliki keterbatasan, sebab alamat IP tidak dapat secara langsung mengungkap identitas individu, sebagaimana pelat nomor kendaraan yang tidak serta-merta menunjukkan siapa pengemudinya (Singer & Friedman, 2014).

Sebagian besar serangan siber bermotif politik di Indonesia ditandai oleh aktivitas peretasan dan perusakan terhadap situs web milik pemerintah. Di samping itu, sebagaimana diungkapkan dalam laporan terbaru, Indonesia juga menghadapi berbagai ancaman siber non-politis, seperti penipuan keuangan berbasis digital, serangan malware terhadap perangkat pribadi, manipulasi melalui teknik rekayasa sosial lewat surel, serta pencurian identitas di platform media sosial. Faktor utama yang memicu kerentanan ini adalah rendahnya tingkat literasi dan kesadaran masyarakat terhadap isu keamanan siber (Pratiwi, F. I., dkk., 2024). Berbagai temuan ini mencerminkan lemahnya sistem pertahanan siber nasional. Dalam konteks tersebut, diplomasi siber muncul sebagai strategi yang krusial. Diplomasi siber merujuk pada upaya negara dalam menjalin kerjasama internasional guna melindungi dan memperkuat kepentingan nasional di ranah digital (Riordan, 2016).

Disrupsi Teknologi dalam Hubungan Internasional

Dalam bukunya, Deibert (2002) menjelaskan bahwa teknologi-teknologi baru yang telah merambah kehidupan kita saat ini telah mempengaruhi banyak lapisan masyarakat termasuk politik dunia. Sebagai salah satu disiplin ilmu terkemuka yang membahas politik dunia.

Kaum realis memandang bahwa kemajuan teknologi tidak secara fundamental mengubah struktur kekuasaan atau relasi sosial, melainkan hanya memodifikasi mekanisme kerja struktur yang telah ada. Dalam perspektif ini, teknologi baru dipahami sebagai instrumen yang memperkuat dan memfasilitasi dinamika perebutan kekuasaan serta menjaga keseimbangan politik global. Namun demikian, pendekatan realisme dinilai kurang mampu menjelaskan peran teknologi

dalam konteks Hubungan Internasional, terutama karena mengabaikan kemunculan aktor non-negara yang peranannya semakin signifikan berkat dukungan teknologi modern (Deibert, 2002).

Di sisi lain, perspektif liberalisme melihat teknologi baru sebagai sarana yang dapat meningkatkan arus informasi, yang pada gilirannya akan mengurangi potensi kesalahpahaman antara aktor internasional terkait identitas atau isu sensitif lainnya yang berpotensi memicu konflik. Dengan demikian, perdamaian internasional diharapkan dapat terwujud. Liberalisme menyederhanakan struktur komunikasi global dengan menciptakan kerangka ideal di mana aktor-aktor berinteraksi secara positif, tanpa memberi penekanan yang signifikan pada kekuasaan dan hubungan sosial antara para aktor tersebut. Hal ini juga menjadi kritik terhadap paham liberal itu sendiri (Deibert, 2002).

Kritik terhadap pandangan ini akan dijawab oleh perspektif Marxisme yang bersifat tetap. Prinsip dasar Marxisme berpendapat bahwa struktur kelas ekonomi dan hubungan-hubungannya dengan cara produksi akan menentukan kelas sosial dan politik. Dalam konteks teknologi baru, Marxisme cenderung memiliki pandangan reduksionis dengan memfokuskan pada kontrol ekonomi atas teknologi baru (seperti telepon, internet, radio, dan televisi). Sebagaimana diilustrasikan oleh Deibert (2002), kepemilikan terhadap teknologi tersebut sangat penting, karena pemilik teknologi akan memanfaatkannya untuk kepentingan mereka sesuai dengan kelas sosial yang telah ditentukan oleh cara produksi yang mereka kendalikan.

Menurut Daniel R. McCarthy, sejalan dengan pandangan yang diutarakan oleh Deibert, disiplin Hubungan Internasional selama ini kurang mendapatkan perhatian yang memadai terkait kemajuan teknologi, meskipun terdapat hubungan yang erat antara keduanya. McCarthy mengemukakan bahwa banyak sarjana Hubungan Internasional yang berupaya mengembangkan pendekatan holistik terhadap dinamika internasional dalam era kemajuan teknologi dengan mengadopsi pendekatan sains dan teknologi (McCarthy, 2017). Argumen McCarthy mengenai integrasi sains, teknologi, dan Hubungan Internasional menunjukkan bahwa politik global pada dasarnya bersifat sosio-teknis, yang berkaitan dengan isu-isu empiris seperti pengelolaan internet, senjata nuklir, dan teknologi pemetaan (McCarthy, 2017).

Teori Hubungan Internasional (HI) dan relevansinya dalam konteks era disrupsi teknologi terus berkembang dan memerlukan kajian lebih lanjut. Meskipun kajian mengenai teknologi dalam HI belum dibahas secara khusus, aspek teknologi telah terintegrasi dalam berbagai kajian lainnya. Seiring berjalannya waktu, dunia semakin menjadi tempat yang dipengaruhi oleh perkembangan teknologi. Meskipun ilustrasi mengenai gangguan akan disampaikan pada sub-bagian berikutnya, perlu ditekankan bahwa penjelasan teoritis akan senantiasa mengikuti perkembangan tersebut, tanpa berupaya untuk memprediksi akibat dari kemajuan teknologi yang sangat pesat.

Menurut Kamus Besar Bahasa Indonesia, diplomasi dipahami sebagai seni dalam berunding yang mencakup kesepakatan antar negara, dengan penekanan pada keterampilan umum yang diperlukan. Di sisi lain, Sir Ernest Satow mendefinisikan diplomasi sebagai

penerapan keterampilan dan kebijaksanaan dalam mengelola hubungan luar negeri antara dua negara yang merdeka. Sementara itu, Harold Nicholson memandang diplomasi sebagai hal yang berkaitan dengan lembaga, departemen, atau individu yang terlibat dalam kebijakan luar negeri, negosiasi, serta upaya untuk mencari solusi terhadap sengketa atau konflik, termasuk lembaga yang menangani urusan atau masalah luar negeri (Alam, 2016).

Diplomasi modern dapat dipahami sebagai profesi serta metode pengelolaan hubungan internasional yang telah mengalami perkembangan sejak abad ke-17 dan ke-18. Salah satu karakteristik utama dari diplomasi modern adalah adanya dukungan yang terstruktur melalui instrumen-instrumen terorganisir, yang mendukung pelaksanaan tugas diplomatik. Instrumen-instrumen tersebut mencakup Kementerian Luar Negeri sebagai pusat pengelolaan politik luar negeri dan perwakilan diplomatik di negara lain yang berfungsi sebagai saluran komunikasi dan implementasi dari kebijakan luar negeri (Louis, A., dkk, 2006).

Konsep Dunia Maya dan Implikasinya

Dunia maya telah mengalihkan berbagai aktivitas manusia (seperti politik, sosial, ekonomi, budaya, spiritual, dan seksual) yang semula berlangsung di dunia nyata ke dalam berbagai bentuk substitusi buatan, sehingga apa yang sebelumnya dapat diselesaikan di dunia nyata kini dapat diselesaikan melalui bentuk-bentuk kepalsuan dalam dunia maya. Dunia maya menciptakan model kehidupan yang dimediasi secara mendalam oleh teknologi, sehingga berbagai fungsi alami kini lebih banyak diambil alih oleh substitusi teknologi, yang dikenal sebagai kehidupan buatan (*artificial life*). Pengaruh dunia maya terhadap kehidupan sosial dapat dilihat pada tiga tingkatan: individu, interaksi antar individu, dan masyarakat. Pertama, pada tingkat individu, dunia maya telah membawa perubahan signifikan dalam pemahaman kita mengenai 'identitas'. Kedua, pada tingkat interaksi antar individu, kemunculan komunitas virtual di dunia maya telah menghasilkan hubungan sosial virtual dalam ruang virtual, seperti belanja virtual, permainan virtual, konferensi virtual, dan seks virtual. Ketiga, pada tingkat masyarakat, dunia maya dipandang mampu menciptakan model masyarakat yang demokratis dan membuka ruang bagi terbentuknya 'komunitas imajiner'. Dalam era yang semakin terhubung secara digital ini, berbagai ruang sosial yang ada di dunia nyata kini dapat digantikan oleh bentuk-bentuk simulasi sosial dalam dunia informasi digital, yang merupakan suatu bentuk simulasi sosial (social simulation). Cyberspace menjadi ruang utama di mana berbagai simulasi sosial tersebut menemukan tempatnya (Piliang, Y. E. S., 2012).

Pemerintah pusat telah memanfaatkan teknologi untuk meningkatkan kinerjanya, termasuk dalam hal layanan publik. Sebagai contoh, Kementerian Luar Negeri Republik Indonesia telah mengimplementasikan pusat komando digital untuk memperkuat diplomasi digital, yang bertujuan meningkatkan efisiensi operasional kementerian (Pernyataan Pers Tahunan Kementerian Luar Negeri Republik Indonesia, 2017). Selain itu, pemerintah daerah Seoul, Korea Selatan, telah memasang layar besar di kantor walikota untuk menampilkan informasi situasional secara real-time mengenai kondisi kota, seperti data kebakaran, keadaan darurat, dan pengaduan warga (Lee, J., & Moon, M. J., 2020). Pemanfaatan teknologi dalam pemerintahan

dan politik umumnya dapat ditemukan di negara-negara dengan prospek *e-governance* yang berkembang pesat, seperti Selandia Baru, Jepang, Inggris, Australia, Kanada, Amerika Serikat, dan Belanda (Dunleavy, dkk. 2007).

Pesatnya adopsi teknologi dalam sektor pemerintahan dan politik telah menyebabkan integrasi dan penyimpanan informasi warga negara, data terkait, serta dokumen rahasia negara dalam sistem cloud online. Hal ini menjadikan informasi yang tersimpan dalam teknologi tersebut berada di bawah yurisdiksi pemerintahan nasional, yang dikenal sebagai dunia virtual (Andress, J., & Winterfeld, S., 2012). Oleh karena itu, diperlukan upaya perlindungan yang sangat ketat terhadap data tersebut, mengingat potensi gangguan yang dapat timbul akibat penempatan teknologi yang tidak tepat, yang berhubungan langsung dengan isu keamanan dan kedaulatan negara.

Serangan siber secara teknis merujuk pada upaya yang dilakukan oleh individu atau kelompok untuk membobol sistem informasi milik pihak lain dengan tujuan memperoleh keuntungan pribadi atau organisasi (Bendovschi, A., 2015). Meskipun sebagian besar pelaku serangan adalah individu atau kelompok kecil, dalam kasus serangan terhadap pemerintah, terdapat beberapa situasi di mana pelaku serangan diduga memperoleh dukungan dari negara lain. Fenomena ini sering kali disebut dengan istilah Advanced Persistent Threat (APT) (Andress, J., & Winterfeld, S., 2012).

Baru-baru ini, Uni Eropa mengungkapkan bahwa kabel diplomatik mereka telah menjadi sasaran penyadapan selama tiga tahun terakhir. Kabel diplomatik merupakan sarana penting bagi para diplomat dalam berkomunikasi, termasuk untuk pertukaran informasi yang bersifat rahasia. Uni Eropa mencurigai bahwa Tiongkok mungkin terlibat dalam serangan siber besar ini (Hasan, Akbar, 2018). Seiring waktu, kasus-kasus serangan siber semakin meningkat baik dalam jumlah maupun frekuensinya. Sebuah laporan yang dikeluarkan oleh Forum Ekonomi Dunia mengenai Risiko Global menunjukkan bahwa serangan siber menjadi salah satu risiko kelima yang paling mungkin berdampak pada negara pada tahun 2019 (Satriawan, I., Elven, T. M. A., & Lailam, T., 2023). Dalam laporan tersebut, responden menyatakan bahwa serangan siber dapat menimbulkan berbagai masalah, seperti: 1) pencurian data dan uang, 2) gangguan operasional, 3) penyebaran berita palsu, dan 4) hilangnya privasi (Satriawan, I., Elven, T. M. A., & Lailam, T., 2023).

Sebaliknya, perang siber dapat dianggap sebagai bentuk disrupsi teknologi yang lebih serius, mengingat dampaknya yang lebih luas dan terkait langsung dengan konteks peperangan. Menurut Adam Segal, perbedaan mendasar antara perang siber dan serangan siber terletak pada akibat yang ditimbulkan, di mana perang siber berpotensi menyebabkan kematian, merusak infrastruktur, serta mengancam kepentingan nasional. Sebaliknya, jika dampaknya tidak sebesar itu, maka insiden tersebut lebih tepat dikategorikan sebagai serangan siber biasa (Beauchamp, 2014).

Dalam upaya mendefinisikan perang siber, beberapa ahli mencoba merujuk pada definisi perang tradisional. Winterfeld dan Andress, misalnya, mengadopsi definisi yang dipaparkan dalam On War, sebuah dokumen yang membahas taktik Perang Napoleon pada tahun 1873, yang menyatakan bahwa "perang adalah duel dalam skala besar, di

mana masing-masing pihak berjuang dengan kekuatan fisik untuk memaksa lawan tunduk pada keinginannya." (Andress, J., & Winterfeld, S., 2012). Berdasarkan definisi ini, perang siber seharusnya dilakukan secara masif. Namun, definisi tersebut tidak sepenuhnya relevan dengan perang siber, mengingat perang siber tidak melibatkan kekuatan fisik. Di sisi lain, Abebe mencoba menghubungkan perang siber dengan definisi perang yang tercantum dalam hukum internasional, khususnya dalam Piagam PBB pada Bab 2 (4) dan Pasal 51, yang menyatakan bahwa perang merupakan penggunaan kekuatan terhadap negara lain dan sebagai upaya pembelaan diri. Abebe menginterpretasikan definisi ini sebagai dasar bagi perang siber yang dapat dimanfaatkan untuk mempertahankan perdamaian internasional. Ia juga mendukung posisi Amerika Serikat dalam konteks perang siber sebagaimana yang dijelaskan oleh Adam Segel sebelumnya (Abebe, 2016).

Bertentangan dengan argumen sebelumnya, kenyataannya adalah bahwa perang siber dapat diartikan sebagai penggunaan teknologi untuk menyebabkan kerusakan fisik secara tidak langsung. Serangan semacam ini tidak selalu mengakibatkan korban jiwa (Singer & Friedman, 2014). Sebagai contoh, serangan Stuxnet pada tahun 2010 berhasil melemahkan sistem keamanan di empat fasilitas nuklir Iran dengan menyerang bagian sentrifugal dari mesin yang berputar. Dalam hal ini, sentrifus dikendalikan oleh perangkat lunak SCADA yang terhubung dengan Programmable Logic Controllers (PLC), perangkat keras yang secara langsung mengatur sentrifus. Stuxnet menyerang sistem ini dengan cara memanipulasi program yang dikirimkan oleh SCADA ke PLC. Hingga saat ini, tidak ada informasi lebih lanjut mengenai pihak atau negara yang bertanggung jawab atas penanaman Stuxnet di fasilitas nuklir Iran. Pemerintah Iran hanya mengonfirmasi bahwa ada elemen mata-mata yang terlibat dalam insiden tersebut (Shakarian, P., Shakarian, J., & Ruef, A. 2013).

Potensi perkembangan kecerdasan buatan (AI) dapat diamati melalui kemampuannya dalam memproses data dalam jumlah besar dengan cepat dan meniru perilaku manusia. Penggunaan senjata otonom secara penuh berpotensi menimbulkan bahaya besar, seperti kecelakaan yang dapat menyebabkan kematian sasaran yang salah, serta berisiko melanggar hukum perang (Sparrow, R., 2007). Senjata otonom ini berpotensi mengubah wajah peperangan tradisional dengan teknologi yang jauh lebih canggih. Oleh karena itu, penting untuk mengantisipasi ancaman perang siber sebagai salah satu bentuk disrupsi teknologi dalam hubungan internasional dan merumuskan langkah-langkah preventif serta responsif guna mengatasi potensi ancaman tersebut.

Perlunya Diplomasi Siber

Menurut Hathaway dan rekan-rekannya (2012), diplomasi siber merujuk pada upaya yang dilakukan oleh suatu negara untuk memengaruhi perilaku aktor negara maupun non-negara di ranah digital melalui instrumen diplomatik. Dalam hal ini, diplomasi siber tidak semata-mata berfokus pada aspek teknis seperti keamanan jaringan, tetapi juga mencakup isu-isu strategis yang lebih luas, seperti pembentukan norma internasional, regulasi aliran data lintas batas, kerjasama dalam penegakan hukum, serta perlindungan terhadap hak-hak digital.

Ketiadaan instrumen internasional yang komprehensif dalam menangani isu-isu tersebut telah menyebabkan ketidakjelasan arah kebijakan dan ketidakefektifan dalam menanggulangi intervensi teknologi dalam hubungan antarnegara. Beberapa kasus bahkan dibiarkan tanpa penyelesaian akibat ketiadaan kerangka hukum internasional yang memadai (Lacy & Prince, 2018). Gagasan mengenai diplomasi siber sendiri muncul dari kesadaran bahwa dunia maya kini memiliki signifikansi yang setara dengan wilayah fisik seperti udara, air, dan daratan bagi suatu negara. Meskipun pendekatan berbasis kebijakan belum tentu menjadi solusi paling ideal, saat ini pendekatan tersebut masih dianggap sebagai praktik terbaik dalam konteks perlindungan siber. Oleh karena itu, kebutuhan akan kolaborasi internasional semakin mendesak, dan diplomasi siber menjadi satu-satunya mekanisme yang memungkinkan penyelesaian isu-isu tersebut secara kolektif (Barrinha & Renard, 2017).

Kerjasama antarnegara menjadi elemen krusial dalam menghadapi potensi serangan dan konflik siber di masa depan. Dalam konteks ini, diplomasi siber berperan sebagai pendekatan alternatif yang memungkinkan terbentuknya kolaborasi internasional dalam mencegah dan merespons berbagai ancaman di dunia maya. Diplomasi siber sendiri dipahami sebagai pemanfaatan instrumen dan kapasitas diplomatik guna melindungi kepentingan nasional yang berkaitan dengan ruang siber (Riordan, 2016). Namun demikian, masih terdapat kebingungan konseptual antara diplomasi siber dan diplomasi digital atau e-diplomasi. Perlu ditegaskan bahwa diplomasi digital merujuk pada penggunaan teknologi informasi dan komunikasi dalam mendukung praktik diplomasi konvensional, sehingga secara substansi berbeda dengan diplomasi siber yang berfokus pada isu-isu strategis di ranah digital (Riordan, 2016).

Keterlibatan diplomat menjadi sangat penting dalam menangani isu-isu keamanan siber, mengingat beberapa alasan strategis. Pertama, ancaman siber berpotensi menimbulkan efek limpahan (*spillover effect*) lintas negara, sehingga diperlukan komunikasi transnasional yang efektif dan penguatan kerjasama internasional secara berkelanjutan. Kedua, peran diplomat dibutuhkan untuk mendorong pengarusutamaan isu keamanan siber ke dalam berbagai forum dan agenda internasional, termasuk dalam kerangka hak asasi manusia, pembangunan, perdagangan global, dan perlindungan hak kekayaan intelektual. Ketiga, diplomat yang memiliki pemahaman terhadap teknologi digital kontemporer akan berperan penting dalam mendiseminasikan isu-isu terkait keamanan dan ancaman siber baik di tingkat pemerintahan nasional maupun kepada publik (Tiirmaa-Klaar, 2013). Tidak seperti konflik konvensional yang dibatasi oleh wilayah geografis, ancaman siber bersifat lintas batas, di mana serangan terhadap infrastruktur digital seperti *e-commerce*, sektor keuangan, dan data pengguna kerap berasal dari yurisdiksi luar negeri. Oleh karena itu, hanya melalui mekanisme diplomasi antarnegara, kerjasama teknis dan hukum lintas batas dapat diwujudkan untuk mengatasi kejahatan siber secara efektif (Hansen & Nissenbaum, 2009). Dalam konteks ini, aktor negara, khususnya diplomat, seharusnya menjadi aktor utama dalam pelaksanaan diplomasi siber, bukan pihak swasta (Tiirmaa-Klaar, 2013).

Pemanfaatan dunia maya dan internet telah memberikan berbagai kontribusi positif yang nyata, seperti maraknya penggunaan

media sosial oleh generasi muda, kemudahan dalam melakukan transaksi daring, peningkatan akses terhadap pendidikan, percepatan pembangunan ekonomi, serta terjadinya akulturasi budaya. Meskipun demikian, kemajuan teknologi ini juga membawa dampak negatif, khususnya dalam bentuk meningkatnya berbagai jenis kejahatan di ranah siber (Primawanti & Pangestu, 2020).

Bangkitnya Diplomasi Siber bagi Keamanan Teknologi *E-commerce* Nasional

Sejarah munculnya diplomasi siber dapat ditelusuri kembali ke tahun 2009, yang ditandai dengan diselenggarakannya Lokakarya Keamanan Siber di Wina sebagai respons atas kepemimpinan Estonia dalam Forum Kerjasama Keamanan di bawah Organisasi Keamanan dan Kerjasama Eropa (OSCE). Dalam forum tersebut, para pimpinan lembaga siber nasional dari berbagai negara berperan layaknya diplomat guna membangun pemahaman bersama mengenai konsep keamanan siber. Inisiatif ini kemudian dilanjutkan dengan serangkaian pertemuan sepanjang tahun 2009 hingga 2010 yang difokuskan pada pembahasan perilaku, pembentukan norma-norma di dunia maya, serta peningkatan kapasitas negara-negara dalam menghadapi ancaman serangan siber (Tiirmaa-Klaar, 2013).

Pada tahun 2010, Amerika Serikat menginisiasi penyelenggaraan sebuah konferensi yang bertujuan untuk merumuskan *Confidence-Building Measures* (CBM) dalam konteks keamanan siber (Tiirmaa-Klaar, 2013). CBM sendiri merupakan instrumen yang digunakan oleh para aktor untuk membangun dan memperkuat rasa saling percaya, khususnya dalam situasi yang melibatkan pihak-pihak yang berpotensi menjadi lawan, dengan tujuan mendorong keterbukaan informasi. Langkah ini menjadi bagian integral dari strategi diplomasi preventif yang bertujuan mencegah eskalasi konflik sejak dini (Harman, 2020).

Dalam Konferensi Seoul tahun 2012, salah satu pendekatan strategis yang diusulkan untuk mengurangi kesenjangan kapasitas siber global adalah pembentukan *Computer Emergency Response Team* (CERT). Inisiatif ini memungkinkan negara-negara berkembang untuk memperkuat kapasitas sibernya melalui pelatihan, alih teknologi, serta pertukaran praktik terbaik melalui jejaring CERT internasional (Tiirmaa-Klaar, 2013).

Di Indonesia, tingkat penetrasi internet mengalami peningkatan sebesar 10% pada tahun 2018, dengan jumlah pengguna yang mencapai sekitar 171 juta orang. Angka ini mencerminkan ketergantungan masyarakat Indonesia terhadap teknologi internet, sehingga berbagai permasalahan yang berkaitan dengan dunia maya pun berpotensi semakin berkembang. Dalam konteks tersebut, keamanan siber menjadi isu strategis yang perlu mendapatkan perhatian utama guna merespons dinamika tersebut secara efektif.

Selain itu, Indonesia juga menghadapi tantangan serius berupa meningkatnya penyebaran informasi palsu (*fake news*) dan penggunaan disinformasi untuk kepentingan politik, yang pada akhirnya dapat mengganggu stabilitas nasional (Paterson, 2019).

Dalam konteks diplomasi siber di tingkat global, posisi Indonesia dapat menjadi

kurang menguntungkan karena adanya persepsi bahwa negara ini belum sepenuhnya menjunjung prinsip dasar kebebasan internet. Hal ini tercermin dari kebijakan pembatasan akses terhadap platform media sosial yang diberlakukan pada Mei 2019, yang tidak hanya menargetkan penyebar informasi palsu, tetapi turut berdampak pada hak-hak digital masyarakat sipil secara keseluruhan. Meskipun demikian, partisipasi Indonesia dalam forum-forum internasional tetap membawa manfaat, terutama dalam hal pertukaran informasi yang dapat meningkatkan kapasitas individu para pemangku kepentingan di bidang keamanan siber, seperti dalam keterampilan pengelolaan internet dan pemahaman terkini mengenai isu-isu siber.

Perkembangan pesat ekonomi digital di Indonesia, yang didorong oleh kemajuan teknologi informasi dan komunikasi, juga menimbulkan tantangan baru di ranah hukum, termasuk perlindungan data pribadi, keamanan siber, serta regulasi terhadap sektor *e-commerce* dan teknologi finansial (*fintech*). Walaupun regulasi yang relevan telah mulai diterapkan, masih terdapat kekosongan hukum serta ketidakpastian normatif yang perlu segera diatasi oleh para pembuat kebijakan dan aparat penegak hukum (Dewi & Sriyanto, 2024).

Dalam hal ini, perlindungan data pribadi menjadi aspek yang sangat krusial, terutama dalam menjamin keamanan transaksi digital dan membangun kepercayaan pengguna. Undang-Undang Perlindungan Data Pribadi (UU PDP) telah memberikan kerangka hukum yang lebih jelas, termasuk pengaturan mengenai sanksi terhadap pelanggaran data. Namun, insiden kebocoran data seperti yang terjadi pada platform Tokopedia menunjukkan masih lemahnya sistem keamanan digital serta implementasi regulasi yang ada. Oleh karena itu, penguatan kapasitas kelembagaan serta peningkatan literasi digital masyarakat menjadi hal yang mendesak (Ardika, 2025).

Perlindungan konsumen dalam kegiatan *e-commerce* merupakan salah satu isu krusial, terutama jika dikaji dari perspektif hukum ekonomi syariah yang menitikberatkan pada prinsip keadilan, transparansi, dan kepastian hukum. Meskipun demikian, penerapan prinsip-prinsip hukum syariah dalam transaksi *e-commerce* masih menemui berbagai hambatan, khususnya yang berkaitan dengan tingkat pemahaman dan kesadaran baik dari sisi konsumen maupun pelaku usaha (Haryono, 2024)

Kesimpulan

Sebagai kesimpulan, kemajuan teknologi telah memberikan kontribusi signifikan bagi kehidupan manusia, namun di sisi lain juga menimbulkan dampak negatif yang tercermin dalam bentuk disrupsi teknologi. Fenomena disrupsi ini tidak hanya memengaruhi sektor ekonomi dan sosial, tetapi juga berdampak langsung pada dinamika politik, tata kelola pemerintahan, serta hubungan internasional. Dalam konteks hubungan antarnegara, disrupsi teknologi, khususnya melalui serangan dan perang siber yang berpotensi terjadi di masa depan, menjadi ancaman serius terhadap keamanan nasional yang harus segera diantisipasi.

Situasi ini berisiko melemahkan posisi tawar Indonesia dalam forum-forum diplomasi siber. Kendati demikian, urgensi diplomasi siber tidak dapat diabaikan. Melalui mekanisme ini, Indonesia dapat memperoleh berbagai manfaat strategis,

seperti alih teknologi, pertukaran informasi, dan peningkatan kapasitas sumber daya manusia di bidang keamanan siber. Saat ini, Indonesia telah menjalin kerjasama dengan Korea Selatan dalam rangka memperkuat kemampuan investigatif terhadap kejahatan siber. Namun, upaya tersebut masih perlu ditingkatkan untuk menjawab tantangan yang kompleks, mengingat karakteristik dunia maya yang melibatkan beragam aktor dan komunitas global. Oleh karena itu, diperlukan pendekatan yang bersifat multipihak dan multidisipliner dalam mengelola isu-isu terkait keamanan siber secara komprehensif.

Dalam kerangka diplomasi siber, perlindungan terhadap ekonomi digital dan sektor *e-commerce* memerlukan penguatan regulasi baik di tingkat nasional maupun internasional, peningkatan sistem keamanan teknologi, serta pengembangan kerjasama lintas sektor dan antarnegara. Langkah ini sangat penting untuk menjamin keamanan transaksi digital, perlindungan data pribadi, keadilan bagi konsumen, serta mendorong pertumbuhan ekonomi digital yang inklusif dan berkelanjutan di tengah transformasi digital global.

Daftar Pustaka

Buku dan E-Book

Andress, J., & Winterfeld, S. (2012). *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Newnes.

Ardipandanto, A., & Budiman, A. (2018). *Dinamika Pelaksanaan Urusan di Bidang Persandian Pemerintah Daerah*. Yayasan Pustaka Obor Indonesia.

Barston, RP (2014). Diplomasi Modern. New York: Routledge.

Beauchamp, Z. (2014). *The Sony hack isn't cyberwar and the US can't really punish North Korea for it*. Vox.

Edition, F. D. (2013). The global competitiveness report 2013–2014.

Harman, B. M. (2020). Evaluating the Impact of Humor Training on Trust Climates within Intact Workgroups (*Doctoral dissertation, Pepperdine University*).

Lacy, M., & Prince, D. (2018). *Securitization and the global politics of cybersecurity*. In Securitisation in the Non-West (pp. 100-115). Routledge.

Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to cyber-warfare: A multidisciplinary approach*. Newnes.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. oup usa.

Artikel Media Online

Hasan, Akbar. (2018). *Jaringan Komunikasi Diplomatik Uni Eropa dan PBB Diretas, Informasi Bocor?* https://www.liputan6.com/global/read/3852634/jaringan-komunikasi-diplomatik-uni-eropa-dan-pbb-diretas-informasi-bocor

Republik Indonesia. Kementrian Luar Negeri. 10 Januari 2017. Negeri Republik Indonesia Retno L. P. Marsudi Tahun 2017." (2017). http://kemlu.go.id/id/pidato/menlu/Documents/PPTM-2017-ID.pdf.

Riordan, S., 2016. *Cyber diplomacy vs. digital diplomacy: a terminological distinction*. USC CPD Blog. http://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction

Prosiding seminar

Louis, A., De Waal, A., & Venter, C. (2006). Named entity recognition in a South African context. In Proceedings of the 2006 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries (pp. 170-179).

Artikel Ilmiah

Abebe, D. (2016). Cyberwar, *International politics, and institutional design*. U. Chi. L. Rev., 83, 1.

Khofifah Hany Amaria, & Roma Ulinnuha. (2023). Transformasi Kesejahteraan Pelaku UMKM melalui Digitalisasi Pembinaan dalam Program "Sibakul Jogja" di Yogyakarta. *ICODEV: Indonesian Community Development Journal*, 4(2), 57–68. https://doi.org/10.24090/icodev.v4i2.9899

Alam, S. (2016). Penggunaan Teknologi Informasi dalam Diplomasi Modern Departemen Luar Negeri RI. *Jurnal International & Diplomacy Universitas Satya Negara Indonesia*, 2(1), 133-144.

Ardika, I. W. C. (2025). Tinjauan Hukum terhadap Perlindungan Data Pribadi di Era Digital: Kasus Kebocoran Data Pengguna Layanan *E-commerce*. *Indonesian Journal of Law and Justice*, 2(3), 11-11.

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. Global Affairs, 3(4-5), 353-364.

Bendovschi, A. (2015). Cyber attacks trends, patterns and security countermeasures. *Procedia Economics and Finance*, 28, 24-31.

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 10(2), 113-128.

Deibert, R. J. (2002). Circuits of power: Security in the internet environment. *Information technologies and global politics: The changing scope of power and governance*, 117.

Dewi, D. K., & Sriyanto, D. (2024). Aspek Hukum dalam Pengaturan Ekonomi Digital: Tantangan dan Peluang di Indonesia. *All Fields of Science Journal Liaison Academia and Sosiety*, 4(2), 73-79.

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New public management is dead—long live digital-era governance. *Journal of public administration research and theory*, 16(3), 467-494.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly,* 53(4), 1155-1175.

Haryono, N. (2024). Perlindungan Hukum bagi Konsumen dalam Transaksi *E-commerce* Berdasarkan Hukum Ekonomi Syariah di Indonesia. *Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora*, 4(2).

Hathaway, O. A., Crootof, R., Levitz, P., & Nix, H. (2012). *The law of cyber-attack*. Calif. L. Rev., 100, 817.

Lee, J., & Moon, M. J. (2020). E-government and digital governance. *In Routledge Handbook of Korean Politics and Public Administration* (pp. 328-344). Routledge.

McCarthy, D. R. (2017). Introduction: Technology in world politics. *In Technology and world politics* (pp. 1-21). Routledge.

Nityasari, A. (2020). Technology Disruptions in International Relations: The Needs for Cyber Diplomacy by Indonesia. Global South Review, 2(1), 36-50.

Paterson, T. (2019). Indonesian cyberspace expansion: a double-edged sword. *Journal of Cyber Policy*, 4(2), 216-234.

Piliang, Y. E. S. (2012). Information and digital society: Information technology and social change. *Journal of Sociotechnology*, 27(11), 143-156.

Pratiwi, F. I., Hennida, C., Soesilowati, S., Berliantin, N., Ekasari, D. Y., Dewi, C. S., & Intan, A. A. (2024). Cybersecurity Challenges in Indonesia: Threat and Responses Analysis. *Perspectives on Global Development and Technology*, 22(3-4), 239-264.

Primawanti, H., & Pangestu, S. (2020). Diplomasi Siber Indonesia Dalam Meningkatkan Keamanan Siber Melalui Association Of South East Asian Nation (Asean) Regional Forum. *Global Mind*, 2(2), 1-15.

Satriawan, I., Elven, T. M. A., & Lailam, T. (2023). I*nternet shutdown in Indonesia: An appropriate response or a threat to human rights*. Sriwijaya Law Review, 7(1), 19-46.

Sparrow, R. (2007). Killer robots. *Journal of applied philosophy*, 24(1), 62-77.

Tiirmaa-Klaar, H. (2013). Cyber diplomacy: Agenda, challenges and mission. *Peacetime Regime for State Activities in Cyberspace*, 509-531.

Valentina, A. L. B. E. R. T. I., Maria, A. R., Carmelo, A. T. T. A. R. D. O., Davide, A. U. T. E. R. I., Ricardo, R. B., Filipe, B. E. S., ... & Grazia, Z. U. L. I. A. N. (2019). The Future of Cities: Opportunities, challenges and the way forward. *JRC Research Reports*, (JRC116711).

This page is intentionally left blank