Review of International Relations
(Jurnal Kajian Ilmu Hubungan Internasional)
Volume 8 Issue 1 (2026), pp. 33-68
doi: 10.24252/rir.v8i1.67123



DIPLOMASI DIGITAL PONTIANAK CSIRT DALAM MENGHADAPI ANCAMAN DUNIA SIBER

Azzomarayosra Wicaksono[1], Ori Fahriansyah[2*], Kalina Alya[3], Muhammad Nirwan Malik Utama[4]
Universitas Tanjungpura[1,2,3,4]

Abstract

Digital transformation has driven a shift in diplomacy practices from traditional models to a more collaborative and network-based approach. Digital diplomacy not only functions as a foreign policy instrument but also as a mechanism to strengthen governance and cybersecurity, while research highlighting the linkage between digital diplomacy and cybersecurity implementation at the regional level is still relatively limited. Local actors such as the Pontianak Computer Security Incident Response Team (Pontianak CSIRT) have an important position in supporting national cyber resilience through multi-level governance. The purpose of this study is to analyze the position and role of the Pontianak Computer Security Incident Response Team (CSIRT) in the framework of Indonesia's digital diplomacy. This study uses a qualitative approach with a descriptive-analytical method based on literature studies. The analysis was carried out with reference to the concepts of digital diplomacy, soft power, and global digital governance. The findings of the study show that CSIRT Pontianak has an important role in the implementation of cybersecurity at the local level, especially in incident handling, digital literacy improvement, and cross-sector collaboration. However, the effectiveness of this role still faces several obstacles, such as limited cybersecurity human resources, coordination between actors that is still centralized, and the lack of regional autonomy in the development of digital diplomacy. This condition shows that there is a gap between the concept of network-based digital diplomacy and implementation practices at the local level which are still hierarchical and administrative. This research contributes to the development of the study of International Relations, especially in expanding the perspective of digital diplomacy from the state level to local actors in the framework of multi-level governance. In addition, this study provides policy recommendations on the importance of strengthening regional CSIRT capacity, decentralizing cybersecurity governance, and building more inclusive digital collaboration in facing global cyber challenges.

*Corresponding Author: Ori Fahriansyah, Universitas Tanjungpura, Indonesia

P-ISSN: 2685-5879; E-ISSN: 2685-421X
Submitted: 17 April 2026; Revised Version: 23 May 2026; Accepted: 26 May 2026;
Published: 15 June 2026

Keywords: digital diplomacy, CSIRT, cybersecurity, digital governance, Indonesia

Abstrak

Transformasi digital telah mendorong perubahan dalam praktik diplomasi dari model tradisional menuju pendekatan yang lebih kolaboratif dan berbasis jaringan. Diplomasi digital tidak hanya berfungsi sebagai instrumen kebijakan luar negeri tetapi juga sebagai mekanisme penguatan tata kelola dan keamanan siber, sementara penelitian yang menyoroti keterkaitan diplomasi digital dengan implementasi keamanan siber di tingkat daerah masih relatif terbatas. aktor lokal seperti Pontianak Computer Security Incident Response Team (Pontianak CSIRT) memiliki posisi penting dalam mendukung ketahanan siber nasional melalui tata kelola multi-level. Tujuan penelitian ini adalah untuk menganalisis posisi dan peran Tim Tanggap Insiden Keamanan Komputer (CSIRT) Pontianak dalam kerangka diplomasi digital Indonesia. Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif-analitis yang didasarkan pada studi literatur. Analisis dilakukan dengan mengacu pada konsep diplomasi digital, soft power, dan tata kelola digital global. Temuan penelitian menunjukkan bahwa CSIRT Pontianak memiliki peran penting dalam implementasi keamanan siber di tingkat lokal, terutama dalam penanganan insiden, peningkatan literasi digital, dan kolaborasi lintas sektor. Namun demikian, efektivitas peran tersebut masih menghadapi beberapa kendala, seperti keterbatasan sumber daya manusia keamanan siber, koordinasi antaraktor yang masih terpusat, serta minimnya otonomi daerah dalam pengembangan diplomasi digital. Kondisi tersebut menunjukkan adanya kesenjangan antara konsep diplomasi digital berbasis jaringan dengan praktik implementasi di tingkat lokal yang masih bersifat hierarkis dan administratif. Penelitian ini berkontribusi pada pengembangan kajian Hubungan Internasional, khususnya dalam memperluas perspektif diplomasi digital dari level negara menuju aktor lokal dalam kerangka multi-level governance. Selain itu, penelitian ini memberikan rekomendasi kebijakan mengenai pentingnya penguatan kapasitas CSIRT daerah, desentralisasi tata kelola keamanan siber, dan pembangunan kolaborasi digital yang lebih inklusif dalam menghadapi tantangan dunia siber global.

Kata Kunci: diplomasi digital, CSIRT, keamanan siber, tata kelola digital, Indonesia.

Pendahuluan

Perkembangan teknologi digital dalam beberapa dekade terakhir telah mendorong transformasi signifikan dalam praktik hubungan internasional, khususnya di bidang diplomasi. Jika sebelumnya diplomasi didominasi oleh interaksi formal

antarnegara melalui jalur diplomatik konvensional, perkembangan teknologi informasi dan komunikasi telah mengubah pola interaksi tersebut menjadi lebih terbuka, cepat, dan berbasis jaringan. Digitalisasi memungkinkan negara untuk tidak hanya berkomunikasi dengan aktor negara lain, tetapi juga berinteraksi secara langsung dengan masyarakat global, organisasi internasional, sektor swasta, dan komunitas digital lintas batas. Perubahan ini melahirkan konsep diplomasi digital (digital diplomacy) sebagai bentuk adaptasi negara terhadap dinamika global di era teknologi informasi.

Dalam perkembangannya saat ini, diplomasi digital tidak lagi terbatas pada penggunaan media sosial atau platform digital oleh suatu negara untuk menyampaikan pesan kebijakan ke luar negeri. Lebih dari itu, diplomasi digital telah berkembang menjadi mekanisme tata kelola global yang melibatkan berbagai aktor dalam pengelolaan isu-isu transnasional Hal ini sejalan dengan konsep multistakeholderisme, yang menekankan pentingnya keterlibatan aktor negara, sektor swasta, komunitas teknis, dan masyarakat sipil dalam mengelola ruang digital, termasuk dalam isu keamanan siber (Raymond & DeNardis, 2015). Dengan demikian, diplomasi digital dapat dipahami sebagai praktik yang tidak hanya bersifat komunikatif, tetapi juga koordinatif dan kolaboratif dalam skala global.

Salah satu isu yang semakin mendesak dalam perkembangan diplomasi digital adalah keamanan siber (cybersecurity). Urgensi ini muncul seiring meningkatnya ketergantungan negara terhadap infrastruktur digital dalam aktivitas pemerintahan, ekonomi, komunikasi, dan pelayanan publik. Kerentanan terhadap serangan siber tidak hanya berdampak pada gangguan teknis, tetapi juga dapat mengancam stabilitas politik, keamanan nasional, serta kepercayaan publik terhadap institusi negara. Dalam konteks hubungan internasional, ancaman siber bahkan telah

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

berkembang menjadi bagian dari kontestasi geopolitik dan instrumen kekuasaan negara di era digital. Berbagai studi empiris menunjukkan bahwa kelalaian dalam pengelolaan keamanan siber dapat menimbulkan konsekuensi serius bagi negara. WannaCry ransomware attack misalnya, menyerang lebih dari 150 negara dan melumpuhkan sistem pelayanan publik, rumah sakit, hingga sektor industri strategis di berbagai wilayah dunia (Greenberg, 2018). Selain itu, serangan terhadap infrastruktur energi Ukraina pada tahun 2015 menjadi bukti bahwa ancaman siber mampu mengganggu layanan publik vital dan digunakan sebagai instrumen tekanan politik antarnegara (Nye, 2017). Di Indonesia sendiri, beberapa insiden seperti kebocoran data pada institusi pemerintah dan serangan ransomware terhadap layanan publik menunjukkan masih lemahnya kesiapan keamanan siber nasional di tingkat institusional maupun daerah.

Literatur mengenai tata kelola digital global juga menegaskan bahwa keamanan siber kini menjadi bagian integral dari diplomasi digital modern. Menurut Joseph S. Nye Jr. (2017), ruang siber telah berkembang menjadi domain kekuasaan baru yang memungkinkan negara maupun aktor non-negara memengaruhi stabilitas politik dan keamanan global tanpa menggunakan kekuatan militer konvensional. Sementara itu, DeNardis (2014) menjelaskan bahwa tata kelola internet dan keamanan siber tidak lagi hanya menjadi isu teknis, melainkan telah berubah menjadi isu politik global yang membutuhkan koordinasi lintas negara dan lintas aktor. Dengan demikian, penguatan kapasitas keamanan siber, termasuk melalui pembentukan CSIRT di tingkat daerah, menjadi bagian penting dari strategi diplomasi digital Indonesia dalam menghadapi dinamika ancaman global di era transformasi digital. Meningkatnya ketergantungan terhadap sistem digital di berbagai sektor kehidupan, seperti pemerintahan, ekonomi, pendidikan, dan pelayanan publik,

telah memperluas potensi kerentanan terhadap ancaman siber. Ancaman tersebut meliputi serangan ransomware, pencurian data (data breach), penyebaran disinformasi digital, hingga gangguan terhadap infrastruktur kritis negara. Menurut laporan World Economic Forum (2023), serangan siber termasuk salah satu risiko global dengan pertumbuhan tercepat karena mampu menimbulkan kerugian ekonomi, gangguan sosial, serta ancaman terhadap stabilitas politik dan keamanan nasional.

Fenomena serangan ransomware menunjukkan bagaimana ancaman siber dapat melumpuhkan sistem layanan publik dan institusi strategis. WannaCry ransomware attack pada tahun 2017 misalnya, menyerang lebih dari 230.000 komputer di sekitar 150 negara dan berdampak pada rumah sakit, perusahaan, serta institusi pemerintahan (Greenberg, 2018). Selain itu, laporan IBM dalam Cost of a Data Breach Report (2023) mencatat bahwa kebocoran data global terus mengalami peningkatan dengan rata-rata kerugian mencapai jutaan dolar per insiden. Kondisi ini menunjukkan bahwa keamanan siber tidak lagi sekadar isu teknis, melainkan telah menjadi isu strategis yang berkaitan dengan ketahanan negara dan tata kelola global. Di sisi lain, perkembangan teknologi digital juga memperbesar risiko penyebaran disinformasi yang dapat memengaruhi stabilitas sosial dan politik. Menurut Bradshaw dan Howard (2019), media digital dan platform media sosial increasingly digunakan sebagai sarana manipulasi opini publik melalui penyebaran informasi palsu secara sistematis. Dalam konteks hubungan internasional, praktik disinformasi bahkan telah menjadi bagian dari kontestasi geopolitik digital antarnegara. Oleh karena itu, penguatan keamanan siber melalui tata kelola digital yang efektif menjadi kebutuhan mendesak bagi negara-negara, termasuk Indonesia, dalam menghadapi kompleksitas ancaman di era transformasi digital. Dalam konteks ini, keamanan siber tidak lagi dipandang

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

sebagai masalah teknis semata, melainkan sebagai bagian integral dari keamanan nasional dan stabilitas global. Oleh karena itu, negara tidak hanya diharuskan untuk memperkuat kapasitas teknis, tetapi juga membangun kerja sama internasional dan tata kelola yang efektif dalam menghadapi ancaman tersebut.

Di Indonesia, upaya menghadapi meningkatnya ancaman siber diwujudkan melalui penguatan diplomasi digital dan pembangunan infrastruktur keamanan siber nasional, salah satunya melalui pembentukan Computer Security Incident Response Team (CSIRT). Pemerintah melalui Badan Siber dan Sandi Negara (BSSN) mendorong pembentukan CSIRT di berbagai tingkatan, baik nasional maupun daerah, sebagai bagian dari strategi penguatan ketahanan siber nasional dan tata kelola keamanan informasi. Kehadiran CSIRT di tingkat daerah, seperti Pontianak CSIRT, mencerminkan adanya upaya desentralisasi pengelolaan keamanan siber sekaligus perluasan keterlibatan aktor lokal dalam tata kelola digital nasional. Namun demikian, keterlibatan aktor lokal dalam diplomasi digital masih menyisakan sejumlah persoalan, baik secara konseptual maupun empiris. Dalam kerangka diplomasi digital, aktor non-negara dan aktor subnasional dipandang memiliki peran penting dalam membangun jejaring kolaborasi lintas sektor dan lintas negara melalui pemanfaatan teknologi digital (Manor, 2016). Selain itu, Bjola dan Holmes (2015) menegaskan bahwa diplomasi digital modern tidak lagi bersifat sepenuhnya hierarkis, melainkan berkembang menuju pola jaringan (network diplomacy) yang melibatkan berbagai aktor di luar pemerintah pusat. Dalam konteks tata kelola digital global, keterlibatan aktor lokal juga dianggap penting untuk menciptakan sistem keamanan siber yang lebih adaptif dan kolaboratif (DeNardis, 2014). Meskipun demikian, praktik implementasi keamanan siber di Indonesia masih menunjukkan kecenderungan koordinasi yang terpusat. CSIRT daerah,

termasuk Pontianak CSIRT, pada dasarnya masih beroperasi dalam struktur kelembagaan yang berada di bawah koordinasi BSSN, sehingga ruang gerak aktor lokal dalam membangun inisiatif diplomasi digital secara mandiri masih relatif terbatas. Kondisi ini menimbulkan pertanyaan mengenai sejauh mana CSIRT daerah dapat diposisikan sebagai aktor dalam diplomasi digital, atau justru hanya berfungsi sebagai pelaksana kebijakan keamanan siber yang dirumuskan di tingkat pusat.

Sejauh ini, penelitian mengenai diplomasi digital Indonesia umumnya berfokus pada diplomasi publik digital, penggunaan media sosial oleh pemerintah, dan kebijakan luar negeri berbasis teknologi (Madu, 2018; Manor, 2019). Sementara itu, studi mengenai CSIRT di Indonesia lebih banyak membahas aspek teknis keamanan informasi, manajemen insiden siber, dan kesiapan infrastruktur digital (najiyya, 2023). Penelitian yang secara khusus menghubungkan peran CSIRT daerah dengan kerangka diplomasi digital dan tata kelola multi-level masih relatif terbatas, khususnya pada konteks pemerintah daerah di Indonesia. Oleh karena itu, penelitian ini berupaya mengisi kekosongan kajian tersebut dengan menganalisis posisi dan peran Pontianak CSIRT dalam diplomasi digital Indonesia serta berbagai tantangan implementasinya di tingkat lokal. Selain itu, terdapat kesenjangan antara draf diplomasi digital yang didasarkan pada diplomasi jaringan dengan realitas implementasinya di tingkat lokal. Konsep diplomasi jaringan menekankan fleksibilitas, kolaborasi, dan pembagian peran antar-faktor, sementara implementasi di lapangan masih menunjukkan kecenderungan top-down dengan keterbatasan dalam hal sumber daya manusia, infrastruktur, dan koordinasi lintas sektor. Kondisi ini juga terkait dengan tantangan dalam tata kelola multi-level, di mana integrasi antara kebijakan nasional dan implementasi lokal belum berjalan secara optimal (Santoso & Putri, 2021).

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

Dari perspektif soft power, diplomasi digital juga memiliki dimensi strategis dalam membangun legitimasi dan kepercayaan publik. Upaya untuk meningkatkan literasi digital, pelatihan keamanan siber, serta kolaborasi internasional dapat dipahami sebagai bagian dari strategi negara untuk memperkuat citra dan kredibilitasnya dalam pengelolaan keamanan siber (Nye, 2004). Namun, efektivitas strategi ini sangat bergantung pada kapasitas aktor lokal dalam menginternalisasi dan mengimplementasikan kebijakan tersebut secara berkelanjutan. Lebih lanjut, dinamika ini menunjukkan bahwa diplomasi digital tidak hanya berkaitan dengan kebijakan luar negeri, tetapi juga mencerminkan kompleksitas tata kelola digital global yang melibatkan interaksi antar berbagai tingkatan pemerintahan. Dalam kerangka ini, aktor lokal seperti Pontianak CSIRT menjadi elemen penting dalam menjembatani kebijakan nasional dengan kebutuhan di tingkat daerah. Namun, keterbatasan struktural yang dihadapi menunjukkan bahwa proses transformasi menuju model diplomasi digital berbasis jaringan yang sepenuhnya masih menghadapi berbagai hambatan.

Berdasarkan latar belakang tersebut, penelitian ini berangkat dari masalah bahwa meskipun diplomasi digital Indonesia memiliki ruang bagi keterlibatan aktor lokal, terdapat hambatan struktural yang membatasi peran mereka sebagai aktor otonom dalam tata kelola serta keamanan siber. Oleh karena itu penting untuk melihat Sejauh mana posisi dan peran diplomasi digital Pontianak CSIRT dalam menghadapi ancaman dunia siber. Adapun penelitian ini bertujuan untuk menganalisis posisi dan peran CSIRT Pontianak dalam kerangka diplomasi digital Indonesia, serta mengidentifikasi kesenjangan antara kerangka teoritis dan implementasi praktis di tingkat lokal.

Kerangka Analisis

Penelitian ini menggunakan tiga konsep utama, yaitu diplomasi digital, soft power, dan tata kelola multi-level (multi-level governance), yang saling berkaitan dalam menganalisis posisi dan peran Pontianak CSIRT dalam keamanan siber Indonesia. Ketiga konsep tersebut tidak dipahami secara terpisah, melainkan sebagai satu kerangka analitis yang menjelaskan hubungan antara kebijakan digital nasional, kapasitas aktor lokal, dan implementasi tata kelola keamanan siber.

1. Diplomasi Digital

   Perkembangan teknologi digital telah mendorong transformasi yang signifikan dalam praktik diplomasi, dari model tradisional yang berpusat pada negara menuju pendekatan yang lebih terbuka, interaktif, dan berbasis jaringan. Dalam hal ini, diplomasi digital tidak hanya merujuk pada penggunaan teknologi komunikasi oleh negara, tetapi juga mencerminkan perubahan dalam cara negara-negara berinteraksi dengan aktor-aktor lain di ranah global. Menurut Manor (2016), diplomasi digital mencakup berbagai praktik yang memungkinkan interaksi dua arah antara negara dan masyarakat, serta mendorong keterlibatan aktor non-negara dalam proses diplomatik. Pendekatan ini menandai pergeseran dari komunikasi satu arah menuju model yang lebih partisipatif, di mana masyarakat tidak lagi sekadar menjadi objek, melainkan juga subjek dalam produksi informasi dan kebijakan. Selain itu, diplomasi digital juga mencerminkan perubahan dalam struktur kekuasaan global, di mana negara tidak lagi menjadi satu-satunya aktor yang dominan. Di era digital, aktor-aktor seperti organisasi internasional, sektor swasta, komunitas teknis, dan bahkan individu memiliki peran masing-masing dalam membentuk dinamika global. Oleh karena itu, diplomasi digital dapat dipahami sebagai praktik-praktik

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

yang adaptif terhadap kompleksitas sistem global yang semakin terhubung.

Konsep diplomasi digital digunakan untuk memahami perubahan praktik diplomasi dari model tradisional menuju pendekatan berbasis jaringan digital yang melibatkan berbagai aktor di luar pemerintah pusat. Dalam konteks ini, Pontianak CSIRT diposisikan sebagai bagian dari jaringan keamanan siber nasional yang mendukung implementasi diplomasi digital Indonesia melalui penanganan insiden siber, literasi digital, dan kolaborasi lintas sektor. Dengan demikian, diplomasi digital menjadi kerangka utama untuk melihat bagaimana teknologi digital menciptakan pola interaksi baru dalam tata kelola keamanan siber.

2. Soft Power

Konsep soft power yang dikemukakan oleh Nye (2004) memberikan perspektif yang penting dalam memahami diplomasi digital. Soft power mengacu pada kemampuan suatu negara untuk memengaruhi pihak lain melalui daya tarik, legitimasi, dan nilai-nilai, bukan melalui kekuatan koersif. Dalam hal diplomasi digital, soft power bukan hanya diwujudkan melalui citra negara, tetapi juga melalui kapasitas kelembagaan dalam menangani isu-isu global, termasuk keamanan siber. Upaya seperti peningkatan literasi digital, pelatihan keamanan siber, serta partisipasi dalam forum internasional dapat dipahami sebagai bentuk strategi soft power yang bertujuan untuk membangun kepercayaan dan kredibilitas. Namun demikian, efektivitas soft power sangat bergantung pada kemampuan implementasi di tingkat lokal. Jika kapasitas aktor lokal terbatas, maka upaya diplomasi digital berpotensi tidak menghasilkan dampak yang optimal. Dengan demikian, terdapat hubungan yang erat antara kapasitas domestik dan efektivitas diplomasi digital dalam membangun pengaruh global.

Konsep soft power digunakan untuk menganalisis bagaimana kapasitas keamanan siber dapat menjadi sumber legitimasi dan kredibilitas negara di era digital. Penguatan CSIRT daerah, peningkatan literasi digital, serta kemampuan respons terhadap ancaman siber dipahami sebagai bagian dari upaya Indonesia membangun citra sebagai negara yang memiliki ketahanan digital. Dalam hal ini, efektivitas diplomasi digital tidak hanya ditentukan oleh kebijakan pusat, tetapi juga oleh kemampuan aktor lokal seperti Pontianak CSIRT dalam mengimplementasikan kebijakan keamanan siber secara efektif.

3. Tata Kelola Digital

   Dari perspektif tata kelola digital global, dunia maya dipahami sebagai arena yang melibatkan berbagai aktor dengan kepentingan yang beragam. DeNardis (2014) menekankan bahwa tata kelola internet dan keamanan siber tidak hanya ditentukan oleh negara, tetapi juga oleh aktor non-negara yang memiliki pengaruh signifikan dalam pengambilan keputusan. Konsep tata kelola multi-level menjelaskan bahwa pengelolaan isu- isu global, termasuk keamanan siber, terjadi di berbagai tingkatan, mulai dari tingkat global hingga nasional dan lokal. Dalam konteks ini, efektivitas kebijakan sangat bergantung pada koordinasi dan integrasi antar tingkatan tersebut (Santoso & Putri, 2021). Namun, dalam praktiknya, seringkali terdapat kesenjangan antara kebijakan tingkat nasional dan implementasi di tingkat lokal. Hal ini disebabkan oleh perbedaan kapasitas, sumber daya, dan prioritas di antara para aktor. Oleh karena itu, memperkuat koordinasi dan pembagian peran merupakan faktor krusial dalam menciptakan tata kelola yang efektif.

   Konsep tata kelola multi-level digunakan untuk menjelaskan hubungan koordinatif antara aktor global, nasional, dan lokal dalam pengelolaan keamanan siber.

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

Konsep ini membantu menjelaskan bagaimana kebijakan keamanan siber nasional yang dirumuskan oleh Badan Siber dan Sandi Negara (BSSN) diterjemahkan dan diimplementasikan di tingkat daerah melalui Pontianak CSIRT. Pendekatan ini juga digunakan untuk menganalisis berbagai kendala implementasi, seperti keterbatasan sumber daya, koordinasi kelembagaan, dan ruang partisipasi aktor lokal dalam diplomasi digital Indonesia.

Dengan demikian, hubungan antar konsep dalam penelitian ini dapat dipahami sebagai berikut: diplomasi digital menjadi konteks transformasi hubungan internasional di era digital; soft power menjelaskan tujuan dan pengaruh yang ingin dibangun melalui kapasitas keamanan siber; sedangkan tata kelola multi-level menjelaskan mekanisme implementasi kebijakan dan interaksi antaraktor dalam sistem keamanan siber nasional. Melalui kerangka ini, penelitian dapat menganalisis sejauh mana Pontianak CSIRT berperan sebagai aktor dalam diplomasi digital Indonesia sekaligus mengidentifikasi faktor-faktor yang membatasi efektivitas perannya di tingkat lokal.

Metode

Penelitian ini menggunakan pendekatan kualitatif sebagaimana dijelaskan oleh John W. Creswell, yang menekankan pemahaman mendalam terhadap fenomena sosial melalui interpretasi makna, konteks, dan relasi antaraktor (Creswell, 2014). Pendekatan ini dipilih karena penelitian berfokus pada analisis diplomasi digital Indonesia dan implementasi tata kelola keamanan siber melalui Pontianak CSIRT yang tidak dapat dijelaskan hanya melalui data kuantitatif. Jenis penelitian yang digunakan adalah deskriptif-analitis. Pendekatan deskriptif digunakan untuk menggambarkan posisi dan peran Pontianak CSIRT dalam sistem keamanan siber nasional,

sedangkan pendekatan analitis digunakan untuk menjelaskan hubungan antara diplomasi digital, soft power, dan tata kelola multi-level dalam implementasi keamanan siber di tingkat lokal.

Penelitian ini menggunakan data sekunder yang diperoleh melalui studi dokumentasi dan studi literatur berbasis digital. Dokumen yang dikumpulkan terdiri atas:

1. Dokumen kebijakan resmi pemerintah terkait keamanan siber dan diplomasi digital, seperti regulasi dan laporan Badan Siber dan Sandi Negara (BSSN);
2. Publikasi resmi pemerintah daerah terkait Pontianak CSIRT;
3. Artikel jurnal ilmiah mengenai diplomasi digital, keamanan siber, dan multi-level governance;
4. laporan organisasi internasional dan lembaga riset; serta
5. Artikel berita dan transkrip pernyataan resmi yang relevan dengan perkembangan keamanan siber di Indonesia.

Pemilihan dokumen dilakukan secara purposif (purposive sampling), yaitu dengan memilih sumber yang memiliki relevansi langsung dengan fokus penelitian. Kriteria pemilihan dokumen meliputi keterkaitan dengan diplomasi digital dan keamanan siber, pembahasan mengenai CSIRT atau tata kelola keamanan siber di Indonesia, kredibilitas sumber, serta keterbaruan publikasi, terutama literatur yang diterbitkan dalam kurun waktu sepuluh tahun terakhir. Dokumen diperoleh melalui basis data akademik seperti Google Scholar, Garuda Kemdikbud, dan Scopus, serta situs resmi lembaga pemerintah terkait.

Analisis data dilakukan menggunakan teknik analisis tematik (thematic analysis). Pada tahap awal, seluruh dokumen

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

dibaca secara menyeluruh untuk mengidentifikasi informasi yang relevan dengan fokus penelitian. Selanjutnya, data dikategorikan ke dalam beberapa tema utama, yaitu Diplomasi digital Indonesia, Kapasitas keamanan siber dan soft power, Tata kelola multi-level, dan Implementasi serta tantangan Pontianak CSIRT.

Setelah proses kategorisasi, data dianalisis secara interpretatif dengan menghubungkan temuan empiris terhadap kerangka teori yang digunakan dalam penelitian. Analisis ini bertujuan untuk melihat bagaimana Pontianak CSIRT diposisikan dalam jaringan tata kelola keamanan siber nasional serta mengidentifikasi faktor-faktor yang membatasi efektivitas perannya dalam diplomasi digital Indonesia. Untuk mengurangi potensi bias penelitian, penelitian ini menggunakan teknik triangulasi sumber dengan membandingkan berbagai jenis dokumen, seperti regulasi pemerintah, artikel akademik, laporan resmi, dan publikasi media. Selain itu, peneliti juga melakukan cross-check antar sumber untuk memastikan konsistensi informasi dan menghindari ketergantungan pada satu sumber data. Dengan demikian, validitas temuan penelitian diupayakan melalui penggunaan sumber yang kredibel, relevan, dan beragam.

Pembahasan

Diplomasi Digital Indonesia

Transformasi digital global telah mendorong berbagai negara untuk mengintegrasikan isu keamanan siber ke dalam strategi diplomatik mereka. Dalam konteks saat ini, diplomasi digital Indonesia berkembang sebagai respons terhadap meningkatnya kompleksitas ancaman siber yang tidak lagi terbatas pada ranah domestik, melainkan juga bersifat lintas batas dan

transnasional. Oleh karena itu, keamanan siber menjadi bagian integral dari agenda diplomasi digital Indonesia, yang tidak hanya berorientasi pada perlindungan sistem nasional, tetapi juga pada penguatan posisi negara dalam tata kelola global. Secara strategis, Indonesia menunjukkan komitmen dalam diplomasi digital melalui partisipasi aktif dalam berbagai forum internasional, seperti ASEAN Digital Ministers Meeting (ADGMIN) yang membahas terkait perkembangan digital dan pemanfaatan teknologi digital dalam peningkatan perekonomian serta kualitas hidup masyarakat ASEAN (Komdigi, 2026), Global Forum on Cyber Expertise (GFCE)) yang merupakan platform global dengan lebih dari 260 anggota (pemerintah, organisasi internasional, sektor swasta, akademisi) untuk memperkuat kapasitas keamanan siber global (TheGFCE.org, 2025), serta Internet Governance Forum (IGF) yang berfokus pada pentingnya melibatkan berbagai multistakeholder kepentingan, mulai dari pemerintah, akademisi, praktisi, dan masyarakat sipil untuk berbagi pengetahuan tentang tata kelola internet (IGF.id, 2024). Hal ini mencerminkan upaya Indonesia untuk bekerja sama secara internasional dalam menghadapi ancaman siber, sekaligus memperkuat kapasitas nasional melalui pertukaran pengetahuan dan praktik terbaik.

Peran diplomasi digital ini semakin penting mengingat tingginya intensitas ancaman siber yang dihadapi Indonesia.Data nasional menunjukkan bahwa ancaman siber di Indonesia terus mengalami peningkatan dalam beberapa tahun terakhir. Menurut Badan Siber dan Sandi Negara (2024), mencatat bahwa sepanjang tahun 2023 terdapat sekitar 403 juta anomali trafik siber di Indonesia, yang sebagian besar didominasi oleh aktivitas malware, trojan, phishing, dan ransomware. Selain itu, pada periode Januari hingga Juli 2024, BSSN kembali mencatat lebih dari 102 juta anomali trafik siber, dengan sekitar 60 persen di antaranya berupa aktivitas malware

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

dan 17 persen aktivitas trojan. Ancaman tersebut tidak hanya bersifat potensial, tetapi juga telah berdampak langsung pada sektor strategis nasional. Laporan BSSN menunjukkan bahwa sektor pemerintahan menjadi salah satu sektor paling rentan terhadap insiden siber sepanjang 2023, termasuk kebocoran data, serangan *ransomware*, dan gangguan layanan digital pemerintah (Katadata,2024). Salah satu kasus yang paling signifikan adalah serangan *ransomware* terhadap Pusat Data Nasional Sementara (PDNS) pada tahun 2024 yang mengganggu layanan lebih dari 230 instansi publik di Indonesia (R3uters, 2024). Jumlah yang tinggi ini menunjukkan bahwa keamanan siber telah menjadi isu strategis yang memerlukan pendekatan komprehensif, tidak hanya melalui kebijakan domestik, tetapi juga melalui kerja sama internasional yang terkoordinasi. Dari perspektif teoretis, perkembangan ini sejalan dengan pandangan bahwa diplomasi digital merupakan bentuk adaptasi negara terhadap perubahan struktur global yang semakin berbasis jaringan (Manor, 2016). Diplomasi tidak lagi dijalankan secara eksklusif oleh aktor negara, melainkan melibatkan berbagai aktor dalam sistem yang saling terhubung . Hal ini juga diperkuat oleh konsep multistakeholderisme yang diusulkan oleh Raymond dan DeNardis (2015), yang menekankan bahwa pengelolaan isu-isu global, termasuk keamanan siber, memerlukan keterlibatan berbagai pihak, seperti pemerintah, sektor swasta, dan masyarakat sipil.

Dalam konteks Indonesia, pendekatan multistakeholder ini tercermin dalam kebijakan penguatan keamanan siber melalui kolaborasi antara pemerintah, lembaga teknis seperti Badan Siber dan Sandi Nasional (BSSN), sektor swasta, serta lembaga pendidikan. Pendekatan ini menunjukkan bahwa diplomasi digital tidak hanya berfungsi sebagai alat komunikasi eksternal, tetapi juga sebagai mekanisme koordinasi internal dalam membangun ketahanan siber nasional. Selain itu, diplomasi digital Indonesia juga memiliki dimensi strategis

dalam kerangka *soft power*. Melalui partisipasi aktif dalam forum global dan pengembangan kapasitas keamanan siber, Indonesia berusaha membangun citra sebagai negara yang memiliki komitmen terhadap keamanan dan stabilitas ruang digital. Hal ini sejalan dengan konsep *soft power* yang menekankan pentingnya daya tarik dan legitimasi dalam membangun pengaruh internasional (Nye, 2004). Dalam konteks ini, keamanan siber menjadi salah satu instrumen penting dalam membangun kredibilitas negara di tingkat global. Namun demikian, orientasi strategis diplomasi digital Indonesia masih menghadapi berbagai tantangan. Salah satu tantangan utama dalam penguatan keamanan siber di Indonesia adalah kesenjangan antara kebijakan nasional dan implementasinya di tingkat daerah. Meskipun pemerintah melalui Badan Siber dan Sandi Negara (BSSN) telah mendorong pembentukan Computer Security Incident Response Team (CSIRT) di berbagai instansi pusat dan pemerintah daerah, kapasitas kelembagaan, sumber daya manusia, dan kesiapan infrastruktur digital antar daerah masih menunjukkan perbedaan yang signifikan. Kondisi ini menyebabkan implementasi kebijakan keamanan siber nasional belum berjalan secara merata di seluruh wilayah Indonesia. Secara empiris, BSSN dalam Laporan Tahunan Monitoring Keamanan Siber menunjukkan bahwa sebagian besar pemerintah daerah masih menghadapi keterbatasan dalam aspek kesiapan keamanan informasi, terutama terkait jumlah personel keamanan siber, pengelolaan insiden, dan integrasi sistem keamanan digital. Selain itu, Indeks Keamanan Informasi (KAMI) yang digunakan untuk mengukur kesiapan keamanan informasi instansi pemerintah menunjukkan bahwa banyak pemerintah daerah masih berada pada kategori "cukup" hingga "kurang" dalam penerapan tata kelola keamanan informasi (BSSN, 2023). Kondisi tersebut memperlihatkan bahwa keberadaan CSIRT di daerah belum selalu diikuti oleh kapasitas

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

operasional yang memadai. Penelitian Santoso dan Putri (2021) juga menunjukkan bahwa implementasi tata kelola keamanan siber di Indonesia masih cenderung terpusat pada pemerintah nasional, sementara pemerintah daerah sering menghadapi kendala berupa keterbatasan anggaran, minimnya tenaga ahli keamanan siber, dan lemahnya koordinasi lintas lembaga. Temuan serupa disampaikan oleh Rahman (2023), yang menjelaskan bahwa beberapa CSIRT daerah di Indonesia masih berfungsi secara administratif dan belum mampu menjalankan respons insiden secara optimal karena keterbatasan infrastruktur dan pelatihan teknis. Hal ini menunjukkan bahwa diplomasi digital Indonesia masih berada pada tahap konsolidasi, khususnya dalam mengintegrasikan berbagai aktor ke dalam sistem tata kelola yang efektif.

Selain itu, koordinasi antar-pihak juga menjadi tantangan dalam implementasi diplomasi digital. Meskipun pendekatan multistakeholder telah diadopsi secara konseptual, dalam praktiknya masih terdapat dominasi aktor negara dalam proses pengambilan keputusan. Kondisi ini menunjukkan bahwa transformasi menuju model diplomasi digital berbasis jaringan belum sepenuhnya terwujud. Dengan demikian, dapat disimpulkan bahwa diplomasi digital Indonesia efektivitasnya sangat bergantung pada kemampuan untuk mengintegrasikan berbagai aktor, memperkuat kapasitas lokal, serta membangun tata kelola yang lebih baik yang inklusif dan kolaboratif. Dalam hal ini, diplomasi digital tidak hanya menjadi instrumen kebijakan luar negeri, tetapi juga menjadi bagian dari proses transformasi tata kelola keamanan siber yang lebih luas.

Peran Pontianak CSIRT dalam Implementasi Diplomasi Digital Lokal

Dalam kerangka diplomasi digital Indonesia, keberadaan Tim Tanggap Insiden Keamanan Komputer (CSIRT) di tingkat daerah merupakan salah satu bentuk konkret dari upaya negara

dalam memperluas kapasitas keamanan siber melalui pendekatan desentralisasi. CSIRT Pontianak, sebagai bagian dari jaringan CSIRT nasional yang dikoordinasikan oleh Badan Siber dan Sandi Nasional (BSSN), memiliki peran strategis dalam menjembatani kebijakan keamanan siber nasional dengan implementasinya di tingkat daerah.

Gambar 1. Pontianak CSIRT



Sumber : Diskominfo Kota Pontianak, 2024

Secara fungsional, Pontianak CSIRT menjalankan sejumlah peran utama yang mencerminkan implementasi keamanan siber di wilayah tersebut. Peran tersebut mencakup penanganan insiden siber, pemantauan ancaman, mitigasi risiko, serta pemulihan sistem yang terdampak. Namun demikian, dalam konteks penelitian ini, relevansi Pontianak CSIRT terhadap diplomasi digital Indonesia tidak dipahami sebagai praktik diplomasi formal sebagaimana dilakukan oleh kementerian luar negeri atau representasi diplomatik negara. Penelitian ini melihat Pontianak CSIRT sebagai bagian dari infrastruktur tata kelola digital nasional yang mendukung agenda diplomasi digital Indonesia di bidang keamanan siber. Dengan kata lain, kontribusi Pontianak CSIRT terhadap diplomasi digital bersifat tidak langsung (indirect contribution), yaitu melalui penguatan ketahanan siber domestik yang menjadi salah satu prasyarat penting dalam membangun kredibilitas digital negara di tingkat internasional. Selain itu,

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

Pontianak CSIRT juga berperan dalam meningkatkan kesadaran dan literasi digital masyarakat melalui kegiatan sosialisasi, pelatihan, dan pendidikan keamanan siber. Kegiatan yang dilakukan meliputi sosialisasi keamanan informasi, simulasi penanganan insiden siber, pelatihan penggunaan sistem digital yang aman, serta edukasi mengenai pentingnya perlindungan data dan kesadaran keamanan digital. Dari sasaran kegiatan mencakup aparatur sipil negara (ASN), operator layanan digital pemerintah, institusi pendidikan, dan masyarakat umum yang menggunakan layanan digital pemerintah daerah. Kemudian kegiatan dilaksanakan di lingkungan Pemerintah Kota Pontianak, sekolah, forum koordinasi pemerintahan daerah, dan platform digital yang digunakan untuk penyebaran informasi publik. Selanjutnya, kegiatan dilakukan secara berkala menyesuaikan program penguatan keamanan informasi daerah dan kebutuhan peningkatan kapasitas digital aparatur pemerintah. Kegiatan ini bertujuan untuk mengurangi risiko serangan siber yang disebabkan oleh rendahnya kesadaran keamanan digital, meningkatkan kesiapsiagaan pengguna sistem informasi, serta mendukung ketahanan siber daerah. Sementara itu, kegiatan dilaksanakan melalui seminar, lokakarya, pelatihan teknis, simulasi respons insiden, penyebaran materi edukasi digital, dan koordinasi antarinstansi dalam penanganan ancaman siber. Fungsi-fungsi ini menunjukkan bahwa CSIRT tidak hanya berperan sebagai entitas teknis, tetapi juga sebagai agen pendidikan dan pencegahan di tingkat lokal. Dalam perspektif keamanan siber, peran ini sejalan dengan temuan Nugraha dan Firmansyah (2021) yang menekankan bahwa CSIRT merupakan komponen penting dalam sistem deteksi dan respons terhadap ancaman siber. Keberadaan CSIRT memungkinkan penanganan insiden secara lebih cepat dan terkoordinasi, sehingga dapat meminimalkan dampak serangan siber terhadap sistem digital pemerintah dan masyarakat.

Namun, jika dilihat dalam konteks diplomasi digital, peran CSIRT Pontianak menjadi lebih kompleks. Diplomasi digital menekankan keterlibatan berbagai aktor dalam jaringan global yang saling terhubung (Manor, 2016). Dalam hal ini, CSIRT Pontianak dapat dipahami sebagai bagian dari jaringan aktor yang berkontribusi dalam tata kelola keamanan siber, baik di tingkat nasional maupun internasional. Keterlibatan dalam pelatihan, lokakarya, dan simulasi yang melibatkan aktor internasional menunjukkan bahwa CSIRT regional memiliki potensi untuk menjadi bagian dari praktik diplomasi digital. Lebih lanjut, dalam kerangka multistakeholderisme, peran Pontianak CSIRT mencerminkan keterlibatan aktor non-tradisional dalam pengelolaan isu-isu global. Raymond dan DeNardis (2015) menekankan bahwa tata kelola digital modern tidak hanya melibatkan negara, tetapi juga berbagai aktor lain yang memiliki kapasitas teknis dan operasional. Dalam konteks ini, CSIRT Pontianak berfungsi sebagai aktor yang berkontribusi secara teknis dalam keamanan jaringan di dunia maya yang lebih luas. Meskipun demikian, hasil studi menunjukkan bahwa peran CSIRT Pontianak masih didominasi oleh fungsi implementatif. Kegiatan yang dilakukan sebagian besar berfokus pada aspek teknis-operasional, seperti penanganan insiden dan pemeliharaan keamanan sistem. Hal ini menunjukkan bahwa CSIRT regional masih berfungsi sebagai pelaksana kebijakan yang dirumuskan di tingkat pusat, bukan sebagai aktor yang memiliki otonomi dalam menentukan arah kebijakan atau strategi diplomasi digital. Kondisi ini sejalan dengan temuan Rahman (2023) yang menunjukkan bahwa implementasi CSIRT di Indonesia masih berorientasi pada fungsi teknis, sehingga perannya dalam diplomasi digital belum berkembang secara optimal. Dengan kata lain, terdapat kesenjangan antara potensi CSIRT sebagai aktor dalam diplomasi digital dengan realitas perannya di lapangan.

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

Selain itu, efektivitas implementasi keamanan siber di tingkat daerah juga dipengaruhi oleh kapasitas kelembagaan dan kesiapan teknis masing-masing CSIRT. Beberapa penelitian menunjukkan bahwa pemerintah daerah di Indonesia masih menghadapi tantangan dalam penguatan keamanan siber, terutama terkait ketersediaan tenaga ahli, pengembangan kapasitas teknis, dan integrasi sistem keamanan informasi (Santoso & Putri, 2021; Rahman, 2023). Kondisi tersebut berpotensi memengaruhi kemampuan CSIRT daerah dalam merespons ancaman siber yang semakin kompleks dan dinamis. Dalam konteks Pontianak CSIRT, keterbatasan tersebut belum dapat diukur secara komprehensif karena minimnya publikasi data kelembagaan yang tersedia secara terbuka, seperti jumlah personel, kapasitas teknis, maupun infrastruktur keamanan siber yang dimiliki. Namun demikian, ketergantungan koordinatif terhadap Badan Siber dan Sandi Negara (BSSN) serta dominannya pola implementasi yang bersifat top-down menunjukkan bahwa kapasitas operasional CSIRT daerah masih sangat dipengaruhi oleh dukungan pemerintah pusat. Oleh karena itu, penelitian ini tidak secara langsung menyimpulkan bahwa Pontianak CSIRT memiliki kelemahan institusional tertentu, melainkan menempatkan isu kapasitas daerah sebagai bagian dari tantangan umum dalam tata kelola keamanan siber Indonesia. Dengan demikian, penting untuk memahami bahwa variasi kapasitas antar daerah dapat memengaruhi efektivitas implementasi diplomasi digital dan keamanan siber di tingkat lokal, meskipun bentuk dan tingkat keterbatasannya dapat berbeda pada setiap CSIRT daerah. Hal ini menunjukkan bahwa penguatan kapasitas menjadi faktor kunci dalam meningkatkan peran CSIRT dalam diplomasi digital.

Dari segi koordinasi, CSIRT Pontianak juga menghadapi tantangan dalam membangun sinergi dengan berbagai multistakeholder, baik di tingkat lokal maupun nasional.

Meskipun pendekatan multistakeholder kepentingan telah diadopsi secara konseptual, namun dalam praktiknya koordinasi antar multistakeholder masih belum optimal. Hal ini mencerminkan bahwa tata kelola keamanan siber di tingkat daerah masih berada pada tahap pengembangan, dengan peran pemerintah pusat yang cukup dominan . Dari perspektif tata kelola multi-level dan pendekatan two-level games yang dikemukakan oleh Robert D. Putnam (1988), penguatan kapasitas keamanan siber di tingkat lokal tidak dapat dipisahkan dari dinamika kebijakan nasional dan tuntutan lingkungan internasional. Putnam menjelaskan bahwa negara beroperasi secara simultan dalam dua arena, yaitu arena domestik dan arena internasional, di mana keduanya saling memengaruhi dan membatasi proses pengambilan kebijakan. Dalam konteks ini, kegiatan Pontianak CSIRT dalam meningkatkan literasi digital, kesadaran keamanan siber, dan koordinasi keamanan informasi dapat dipahami sebagai bagian dari upaya pemerintah untuk memperkuat legitimasi dan kesiapan domestik dalam menghadapi tantangan keamanan siber global. Melalui perspektif tersebut, publik domestik menjadi penting karena tingkat kesiapan dan dukungan internal akan memengaruhi efektivitas implementasi kebijakan keamanan siber nasional. Dengan kata lain, keberhasilan diplomasi digital Indonesia tidak hanya ditentukan oleh keterlibatan dalam forum internasional atau pembangunan citra eksternal, tetapi juga oleh kemampuan pemerintah membangun kapasitas institusional dan kepercayaan di tingkat domestik. Oleh karena itu, peran Pontianak CSIRT lebih tepat dipahami sebagai bagian dari mekanisme penguatan tata kelola keamanan siber nasional yang mendukung posisi Indonesia dalam menghadapi dinamika keamanan digital global.

Tabel 1. Peran dan Fungsi Pontianak CSIRT Dalam Keamanan Siber Dan Diplomasi Digital

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

No.	Dimensi Peran	Bentuk Implementasi	Indikator Kegiatan
1	Respons Insiden Siber	Deteksi, analisis, dan penanganan insiden keamanan digital	Penanganan laporan insiden dan mitigasi ancaman
2	Pencegahan & Mitigasi	Pemetaan risiko dan identifikasi kerentanan sistem	Audit keamanan dan evaluasi sistem digital
3	Literasi & Edukasi Digital	Sosialisasi dan pelatihan keamanan siber	Edukasi kepada ASN, masyarakat, dan pelaku usaha
4	Kolaborasi Multiaktor	Kerja sama dengan BSSN, pemerintah daerah, dan sektor lain	Pembentukan CSIRT dan koordinasi lintas sektor
5	Integrasi Nasional	Keterlibatan dalam jaringan CSIRT nasional	Partisipasi dalam peluncuran CSIRT nasional (32 daerah)
6	Perlindungan Layanan Publik	Pengamanan sistem pemerintahan berbasis elektronik	Monitoring sistem layanan digital pemerintah
7	implementasi tata kelola keamanan siber	Keterlibatan dalam jaringan keamanan siber nasional	Partisipasi dalam pelatihan dan forum kolaboratif

Sumber: https://csirt.pontianak.go.id/

Secara keseluruhan, peran Pontianak CSIRT dalam pelaksanaan diplomasi digital lokal menunjukkan adanya kontribusi dalam memperkuat keamanan siber di tingkat daerah. Namun, kontribusi tersebut masih terkendala oleh batasan struktural serta keterbatasan otonomi dan ruang gerak CSIRT sebagai aktor dalam diplomasi digital. Dengan demikian, dapat disimpulkan bahwa Pontianak CSIRT memiliki posisi strategis sebagai penghubung antara kebijakan nasional dan implementasi lokal dalam keamanan siber. Namun, agar dapat berperan secara optimal dalam diplomasi digital, diperlukan penguatan kapasitas, peningkatan koordinasi multi-aktor, serta

transformasi tata kelola menuju model yang lebih kolaboratif dan berbasis jaringan.

Intensitas Ancaman Siber: Perbandingan Nasional dan Lokal

Meningkatnya ketergantungan terhadap sistem digital di berbagai sektor kehidupan telah menyebabkan meningkatnya ancaman siber yang signifikan, baik di tingkat global, nasional, maupun lokal. Dalam konteks Indonesia, intensitas ancaman siber menunjukkan tren yang terus meningkat , yang menuntut adanya respons strategis tidak hanya di tingkat pusat, tetapi juga di daerah. Secara nasional, lanskap keamanan siber Indonesia menunjukkan tingkat kerentanan yang cukup tinggi . Berdasarkan laporan Badan Siber dan Kriptografi Nasional (BSSN), Indonesia mencatat ratusan juta aktivitas lalu lintas siber yang tidak normal setiap tahunnya, yang mencakup berbagai bentuk serangan seperti *malware, phishing, dan ransomware*.

Dalam laporan keamanan siber tahun 2024, Badan Siber dan Sandi Negara mencatat lebih dari 330 juta aktivitas lalu lintas siber yang tidak normal, termasuk sekitar 26 juta aktivitas phishing dan lebih dari 500 ribu serangan ransomware (BSSN, 2024). Angka tersebut menunjukkan bahwa ancaman siber di Indonesia tidak lagi bersifat sporadis, melainkan telah menjadi ancaman sistemik yang berpotensi memengaruhi layanan publik dan infrastruktur digital pemerintah daerah. Dalam konteks ini, keberadaan CSIRT daerah, termasuk Pontianak CSIRT, menjadi penting sebagai garda awal (first responder) dalam mendeteksi dan menangani insiden keamanan siber di tingkat lokal. Bagi Pontianak CSIRT, tingginya jumlah ancaman siber nasional tersebut memiliki beberapa implikasi penting. Pertama, meningkatnya volume serangan menunjukkan bahwa pemerintah daerah tidak dapat lagi bergantung sepenuhnya pada respons terpusat dari pemerintah nasional. Pontianak CSIRT dituntut memiliki kapasitas deteksi dini dan respons

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

cepat terhadap potensi serangan yang dapat mengganggu sistem layanan publik daerah. Ancaman seperti phishing misalnya, secara langsung berkaitan dengan keamanan akun pemerintahan dan potensi kebocoran data instansi daerah, sehingga membutuhkan pemantauan dan edukasi keamanan digital secara berkelanjutan. Kedua, tingginya angka serangan ransomware menunjukkan pentingnya kesiapan infrastruktur keamanan informasi di tingkat daerah. Dalam praktiknya, Pontianak CSIRT perlu memastikan adanya mekanisme backup recovery, pembaruan sistem keamanan, serta prosedur penanganan insiden yang jelas untuk meminimalkan dampak serangan terhadap layanan digital pemerintah daerah. Dengan kata lain, data ancaman siber nasional tersebut menunjukkan bahwa fungsi Pontianak CSIRT tidak hanya bersifat administratif, tetapi juga berkaitan langsung dengan ketahanan operasional sistem pemerintahan daerah. Ketiga, besarnya skala ancaman nasional memperlihatkan bahwa kapasitas respons CSIRT daerah menjadi faktor penting dalam efektivitas tata kelola keamanan siber nasional. Semakin tinggi intensitas ancaman siber, semakin besar kebutuhan terhadap koordinasi antara CSIRT daerah dan Badan Siber dan Sandi Negara dalam berbagi informasi ancaman (threat intelligence), mitigasi risiko, dan respons insiden. Oleh karena itu, data ancaman siber nasional tidak hanya menggambarkan kondisi keamanan digital Indonesia secara umum, tetapi juga menjelaskan mengapa penguatan kapasitas Pontianak CSIRT menjadi relevan dalam implementasi keamanan siber di tingkat lokal.

Selain itu, Indonesia juga menghadapi ancaman serius dalam bentuk kebocoran data. BSSN mencatat ratusan kasus kebocoran data yang melibatkan lembaga pemerintah dan sektor swasta, yang menunjukkan masih adanya kelemahan sistem perlindungan data di berbagai sektor. Angka yang tinggi ini menunjukkan bahwa ancaman siber di Indonesia tidak

hanya bersifat teknis, tetapi juga berdampak pada berbagai aspek ekonomi, sosial, dan politik.

Di tingkat lokal, kondisi serupa juga terlihat, meskipun dengan skala yang lebih terbatas . Di Provinsi Kalimantan Barat, misalnya, tercatat sebanyak 1.474.148 serangan siber pada periode Januari hingga Juli 2024 (Dinas Komunikasi dan Informatika Provinsi Kalimantan Barat, 2024). Angka yang banyak ini menunjukkan bahwa wilayah tersebut juga menjadi sasaran dalam lanskap ancaman siber nasional. Jika dibandingkan, data nasional dan lokal menunjukkan pola yang menarik. Di satu sisi, skala ancaman nasional jauh lebih besar, mencerminkan kompleksitas sistem digital yang lebih luas. Namun di sisi lain, intensitas serangan di tingkat lokal menunjukkan bahwa wilayah tersebut tidak kebal terhadap ancaman siber, bahkan sering menjadi titik lemah dalam sistem keamanan nasional. Dari perspektif tata kelola digital, kondisi ini mencerminkan adanya ketimpangan antara kapasitas dan kebutuhan. Sementara ancaman terus meningkat, kemampuan daerah dalam merespons masih dibatasi oleh faktor-faktor seperti sumber daya manusia, infrastruktur, dan anggaran. Sejumlah data dan laporan empiris lain juga menunjukkan bahwa penguatan keamanan siber di Indonesia masih menghadapi kendala serius terkait sumber daya manusia, infrastruktur, dan anggaran, terutama di tingkat pemerintah daerah. Kepala Badan Siber dan Sandi Negara (BSSN), Hinsa Siburian, menyatakan bahwa Indonesia masih mengalami kekurangan tenaga ahli keamanan siber. Menurutnya, kebutuhan nasional mencapai sekitar 8.000 tenaga keamanan siber per tahun, sementara lembaga pendidikan yang dimiliki BSSN hanya mampu menghasilkan sekitar 100 lulusan setiap tahun. Kekurangan tersebut tidak hanya berdampak pada instansi pusat, tetapi juga memengaruhi kapasitas kementerian, lembaga, dan pemerintah daerah dalam membangun sistem keamanan siber yang memadai (KompasTV, 2024). Selain

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

keterbatasan SDM, persoalan infrastruktur dan anggaran juga menjadi tantangan utama. Dalam kasus serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) tahun 2024, pemerintah mengakui bahwa banyak instansi belum memiliki sistem backup data yang memadai karena keterbatasan anggaran dan rendahnya prioritas terhadap keamanan siber. Hinsa Siburian bahkan menyebut bahwa lemahnya tata kelola dan tidak adanya sistem pencadangan data menjadi salah satu penyebab utama besarnya dampak serangan tersebut (Kompas.id, 2024). Temuan serupa juga terlihat di tingkat daerah. Dalam evaluasi keamanan siber Pemerintah Provinsi Sulawesi Tenggara bersama BSSN pada tahun 2024, peningkatan infrastruktur dan sumber daya manusia keamanan siber menjadi salah satu isu utama yang dibahas. Hal ini menunjukkan bahwa tantangan kapasitas keamanan siber daerah tidak hanya terjadi pada satu wilayah tertentu, tetapi merupakan persoalan yang lebih luas dalam implementasi tata kelola keamanan siber nasional (Datasultra, 2024).

Lebih lanjut, tingginya jumlah serangan siber juga memperkuat relevansi pendekatan multistakeholder dalam keamanan siber. Raymond dan DeNardis (2015) menekankan bahwa pengelolaan ruang digital memerlukan keterlibatan berbagai aktor, karena karakteristik ancaman yang kompleks dan lintas batas. Dalam konteks ini, pemerintah daerah, lembaga teknis seperti CSIRT, serta sektor swasta dan publik memiliki peran saling melengkapi dalam menciptakan sistem keamanan yang efektif. Selanjutnya , intensitas ancaman siber juga berkaitan erat dengan rendahnya tingkat literasi digital di masyarakat. Kurangnya pemahaman tentang keamanan digital dapat meningkatkan kerentanan terhadap serangan, terutama yang berbasis rekayasa sosial seperti phishing. Putri dan Hidayat (2021) menekankan bahwa literasi digital merupakan faktor penting dalam membangun ketahanan siber pada tingkat individu dan masyarakat.

Berdasarkan penjelasan di atas, perbandingan analisis antara tingkat nasional dan lokal menunjukkan bahwa ancaman siber di Indonesia bersifat sistemik dan memerlukan pendekatan terpadu. Diplomasi digital di berperan penting dalam hal ini. Diplomasi digital berfungsi sebagai mekanisme yang memungkinkan koordinasi lintas sektor dan lintas tingkat, sehingga dapat memperkuat kapasitas nasional sekaligus mengurangi kesenjangan di tingkat lokal dan memungkinkan Indonesia bersaing di kancah global.

Secara umum, tingginya intensitas ancaman siber, baik di tingkat nasional maupun lokal, menegaskan urgensi penguatan sistem keamanan siber yang didasarkan pada kolaborasi dan integrasi. Dalam konteks ini, kehadiran CSIRT di wilayah tersebut, termasuk CSIRT Pontianak, sangat penting sebagai garda terdepan dalam menanggapi ancaman serta sebagai penghubung antara kebijakan nasional dan implementasi lokal.

Kesimpulan

Temuan dalam penelitian ini menunjukkan bahwa diplomasi digital Indonesia telah mengalami perkembangan sebagai respons terhadap meningkatnya kompleksitas tantangan global, khususnya di bidang keamanan siber. Melalui keterlibatan dalam berbagai forum internasional serta penguatan kebijakan nasional, diplomasi digital tidak hanya berfungsi sebagai instrumen komunikasi ke luar negeri, tetapi juga sebagai bagian dari upaya strategis dalam membangun tata kelola keamanan siber yang lebih komprehensif. Di tingkat lokal, keberadaan Pontianak Computer Security Incident Response Team (CSIRT) mencerminkan implementasi konkret dari diplomasi digital Indonesia dalam memperkuat ketahanan siber. Pontianak CSIRT memainkan peran penting dalam penanganan insiden, mitigasi ancaman, peningkatan literasi digital, serta kolaborasi lintas sektor. Peran ini menunjukkan bahwa aktor lokal

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

memiliki kontribusi yang signifikan dalam mendukung agenda keamanan siber nasional.

Temuan penelitian ini juga menunjukkan bahwa implementasi keamanan siber daerah masih didominasi oleh pola koordinasi yang bersifat top-down melalui struktur kelembagaan Badan Siber dan Sandi Negara (BSSN). Dalam praktiknya, Pontianak CSIRT berperan terutama sebagai pelaksana teknis kebijakan keamanan siber nasional, sementara ruang inisiatif daerah dalam membangun kolaborasi keamanan digital secara mandiri masih relatif terbatas. Kondisi tersebut menunjukkan bahwa tata kelola keamanan siber Indonesia masih cenderung terpusat, meskipun ancaman siber increasingly bersifat lintas sektor, lintas wilayah, dan membutuhkan respons yang lebih fleksibel. Model tata kelola yang terlalu terpusat memiliki beberapa keterbatasan. Pertama, ketergantungan tinggi terhadap koordinasi pusat dapat memperlambat respons daerah terhadap ancaman siber yang bersifat cepat dan dinamis. Kedua, variasi kapasitas dan kebutuhan daerah sering kali tidak sepenuhnya terakomodasi dalam pendekatan kebijakan nasional yang seragam. Ketiga, pola top-down berpotensi membatasi pengembangan kapasitas lokal dan partisipasi aktor non-pemerintah dalam keamanan siber daerah.

Dalam literatur tata kelola digital global, pendekatan berbasis jaringan (network governance) dan multi-stakeholder governance increasingly dipandang lebih adaptif terhadap kompleksitas ruang siber. Laura DeNardis (2014) menegaskan bahwa keamanan siber tidak dapat dikelola hanya oleh negara, tetapi membutuhkan keterlibatan pemerintah daerah, sektor swasta, komunitas teknis, akademisi, dan masyarakat sipil. Sementara itu, Bjola dan Holmes (2015) menjelaskan bahwa diplomasi digital modern berkembang menuju pola interaksi horizontal yang menekankan kolaborasi lintas aktor dibandingkan kontrol hierarkis tradisional. Dalam konteks

Pontianak CSIRT, pendekatan berbasis jaringan dapat diwujudkan melalui penguatan koordinasi horizontal antar-CSIRT daerah, peningkatan kerja sama dengan perguruan tinggi dan komunitas teknologi lokal, serta pengembangan mekanisme berbagi informasi ancaman siber secara lebih terbuka. Model ini dinilai lebih adaptif karena memungkinkan respons keamanan siber yang lebih cepat, kontekstual, dan sesuai dengan kebutuhan daerah. Selain itu, pelibatan aktor lokal juga dapat memperkuat kapasitas deteksi dini dan meningkatkan kesadaran keamanan digital masyarakat secara lebih partisipatif. Dengan demikian, kebutuhan terhadap tata kelola keamanan siber yang lebih desentralistis tidak dimaksudkan untuk mengurangi peran pemerintah pusat, melainkan untuk menciptakan pola koordinasi yang lebih kolaboratif dan fleksibel antara pemerintah pusat dan daerah. Dalam kerangka diplomasi digital, pendekatan berbasis jaringan menjadi penting karena ancaman siber increasingly menuntut keterlibatan multiaktor dan kemampuan respons yang tidak sepenuhnya dapat ditangani melalui struktur birokrasi terpusat.

Dalam perspektif yang lebih luas, temuan studi ini menegaskan bahwa efektivitas diplomasi digital Indonesia tidak hanya ditentukan oleh partisipasi dalam forum global, tetapi juga oleh kemampuan untuk mengintegrasikan aktor lokal dalam tata kelola yang lebih baik yang inklusif dan kolaboratif. Oleh karena itu, diperlukan penguatan kapasitas CSIRT regional, peningkatan koordinasi multi-aktor, serta pengembangan kebijakan yang lebih desentralisasi guna mendorong transformasi menuju model diplomasi digital berbasis jaringan. Dengan demikian, diplomasi digital Indonesia masih berada pada tahap transisi, di mana upaya untuk membangun sistem keamanan siber terintegrasi telah berjalan, namun belum sepenuhnya mampu mengatasi kesenjangan antara kebijakan nasional dan implementasi lokal.

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

Penguatan peran aktor lokal seperti CSIRT Pontianak menjadi kunci dalam meningkatkan efektivitas diplomasi digital sekaligus memperkuat ketahanan siber nasional di masa yang akan datang.

Meskipun demikian, penelitian ini memiliki beberapa keterbatasan. Pertama, penelitian ini menggunakan pendekatan studi literatur sehingga sangat bergantung pada ketersediaan dokumen dan data sekunder yang dapat diakses secara publik. Keterbatasan tersebut menyebabkan penelitian belum mampu menggambarkan kondisi internal Pontianak CSIRT secara lebih mendalam, seperti kapasitas sumber daya manusia, infrastruktur teknis, mekanisme operasional, dan evaluasi efektivitas penanganan insiden siber. Kedua, penelitian ini belum menggunakan data primer seperti wawancara dengan pengelola CSIRT, pejabat pemerintah daerah, atau pihak Badan Siber dan Sandi Negara sehingga analisis mengenai praktik koordinasi dan tantangan implementasi masih bersifat terbatas. Ketiga, penelitian ini hanya berfokus pada satu kasus daerah sehingga belum dapat menggambarkan variasi implementasi CSIRT di daerah lain di Indonesia. Berdasarkan keterbatasan tersebut, penelitian selanjutnya disarankan untuk menggunakan pendekatan empiris yang lebih mendalam melalui wawancara, observasi kelembagaan, atau studi komparatif antar-CSIRT daerah di Indonesia. Selain itu, penelitian mendatang juga dapat mengeksplorasi hubungan antara keamanan siber daerah dengan diplomasi siber internasional, kolaborasi lintas negara, maupun keterlibatan sektor non-pemerintah dalam tata kelola keamanan digital Indonesia. Dengan demikian, kajian mengenai diplomasi digital dan keamanan siber dapat berkembang tidak hanya pada aspek kebijakan nasional, tetapi juga pada dinamika implementasi dan kapasitas aktor lokal di era digital.

Daftar Pustaka

Badan Siber dan Sandi Negara. (2023). Laporan Tahunan Monitoring Keamanan Siber Indonesia 2023. Jakarta: BSSN.

Badan Siber dan Sandi Negara. (2024). Laporan kinerja keamanan siber nasional. BSSN.

Badan Siber dan Sandi Negara. (2024, June 27). Januari–Juni 2024 terdapat 91.413.397 anomali trafik didominasi aktivitas malware. FIN News.

Bjola, C., & Holmes, M. (2015). Digital Diplomacy: Theory and Practice. Routledge.

Bradshaw, S., & Howard, P. N. (2019). The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation. Oxford Internet Institute.

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). Sage Publications.

Datasultra. (2024, October 16). Diskominfo Sultra gelar evaluasi keamanan siber bersama BSSN bahas peningkatan infrastruktur dan SDM.

DeNardis, L. (2014). The global war for internet governance. Yale University Press.

Dinas Komunikasi dan Informatika Provinsi Kalimantan Barat. (2024). Samuel tegaskan pentingnya CSIRT dan peningkatan nilai indeks KAMI. https://diskominfo.kalbarprov.go.id/berita/samuel-tegaskan-pentingnya-csirt-dan-peningkatan-nilai-indeks-kami/

Greenberg, A. (2018). Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. Doubleday.

IBM. (2023). Cost of a Data Breach Report 2023.

Katadata. (2024). Government the most vulnerable sector to cyber incidents. Databoks.

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama

Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). Laporan tahunan keamanan siber.

Kompas TV. (2024). Kepala BSSN sebut Indonesia kurang SDM keamanan siber.

Kompas. (2024, June 27). PDN lumpuh, BSSN ungkap tak ada backup data jadi masalah utama. Kompas.id

Kurniawan, D. (2022). Kolaborasi multiaktor dalam tata kelola digital. Jurnal Kebijakan Publik, 13(1), 45–60.

Madu, L. (2018). Indonesia's Digital Diplomacy: Problems and Challenges.

Manor, I. (2016). Are We There Yet: Have MFAs Realized the Potential of Digital Diplomacy? Brill Research Perspectives.

Manor, I. (2019). The Digitalization of Public Diplomacy. Palgrave Macmillan.

Najiyya, A., & Wulandari, S. (2023). Eksplorasi implementasi kebijakan pembentukan Computer Security Incident Response Team (CSIRT) di Kementerian Perdagangan: Sebuah studi kualitatif. JRAM (Jurnal Riset Akuntansi Multiparadigma), 10(1), 50–55. https://doi.org/10.30743/akutansi.v10i1.7246

Nugraha, A., & Firmansyah, M. (2021). Peran CSIRT dalam keamanan siber. Jurnal Keamanan Siber Indonesia, 3(1), 1–12.

Nye, J. S. (2004). Soft power. Public Affairs.

Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. International Security, 41(3), 44–71.

Pemerintah Kota Pontianak. (2022). Peraturan wali kota Pontianak tentang sistem pemerintahan berbasis elektronik.

Putri, R. A., & Hidayat, T. (2021). Literasi digital dan ketahanan siber. Jurnal Komunikasi Pembangunan, 19(2), 200–214.

Rahman, F. (2023). Implementasi CSIRT di Indonesia: Tantangan dan kesiapan daerah. Jurnal Teknologi Informasi dan Keamanan Siber, 12(1), 45–58.

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. International Theory, 7(3), 572–616. https://doi.org/10.1017/s1752971915000081

Reuters. (2024, June 28). Bulk of Indonesia data hit by cyberattack not backed up, officials say.

Robert D. Putnam. (1988). Diplomacy and domestic politics: The logic of two-level games. International Organization, 42(3), 427–460. https://doi.org/10.1017/S0020818300027697

Santoso, H., & Putri, N. E. (2021). Multi-level governance keamanan siber. Jurnal Administrasi Publik, 18(3), 300–315.

Setiawan, B. (2022). Strategi keamanan siber. Jurnal Informatika, 7(2), 89–102.

World Economic Forum. (2023). Global Risks Report 2023.

Copyright (c) 2026 Azzomarayosra Wicaksono, Ori Fahriansyah, Kalina Alya, Nirwan Malik Utama