STRATEGI PERTAHANAN SIBER INDONESIA DALAM MENGHADAPI ANCAMAN KEBOCORAN DATA DAN DISINFORMASI : ANALISIS KASUS DUKCAPIL 2023-2024

Fathiya Mayla Shafira[1], Satria Anindya[2], Zidni Alfiyan Rosadi[3], Dhandy Rahmat Lingga[4], Jerry Indrawan[5]

[1,2,3,4,5]*Universitas Pembangunan Nasional 'Veteran' Jakarta*
E-mail : 2210413174@mahasiswa,upnvj.ac.id[1], 2210413196@mahasiswa.upnv.ac.id[2], 2210413016@mahasiswa.upnvj.ac.id[3], 2410413156@mahasiswa.upnvj.ac.id[4], jerry.indrawan@upnvj.ac.id[5]

ABSTRAK

Abstrak penelitian ini menganalisis strategi pertahanan siber Indonesia menghadapi ancaman kebocoran data massal dan disinformasi melalui studi kasus Dukcapil 2023-2024, di mana 337 juta data pribadi bocor via BreachForums, memicu penipuan identitas dan hoaks medsos yang mengancam stabilitas nasional. Menggunakan pendekatan kualitatif analisis kasus dengan data sekunder dari BSSN, Kemendagri, dan laporan media, penelitian mengevaluasi efektivitas RAN Kamsiber 2024-2028, UU PDP 2022, Peraturan BSSN No. 5/2024, serta RUU KKS 2025 dalam pencegahan, deteksi, dan respons hybrid threat yang menggabungkan peretasan teknis dengan manipulasi informasi. Temuan mengungkap kelemahan seperti koordinasi lintas lembaga lemah, defisit talenta digital, dan literasi siber rendah, yang memperburuk dampak kebocoran terhadap kepercayaan publik dan demokrasi. Penelitian merekomendasikan model adaptif berbasis Zero Trust architecture, active cyber defense, optimalisasi CSIRT di 264 daerah, serta kampanye literasi massal untuk ketahanan siber nasional yang lebih tangguh. Hasil ini berkontribusi pada penguatan kebijakan transformasi digital Indonesia di era ancaman siber

Kata Kunci : *Pertahanan Siber, Kebocoran Data, Disinformasi, Dukcapil*

ABSTRACT

This study analyzes Indonesia's cyber defense strategies against massive data breaches and disinformation threats through the Dukcapil 2023-2024 case study, where 337 million personal records leaked via BreachForums, triggering identity fraud and social media hoaxes that threaten national stability. Employing a qualitative case analysis approach with secondary data from BSSN, Kemendagri, and media reports, the research evaluates the effectiveness of RAN Kamsiber 2024-2028, UU PDP 2022, BSSN Regulation No. 5/2024, and the proposed RUU KKS 2025 in prevention, detection, and response to hybrid threats combining technical hacking with information manipulation. Findings reveal weaknesses such as poor inter-agency coordination, digital talent shortages, and low cyber literacy, exacerbating the breach's impact on public trust and democracy. The study recommends an adaptive model based on Zero Trust architecture, active cyber defense, optimization of CSIRT across 264 regions, and mass literacy campaigns to bolster national cyber resilience. These results contribute to strengthening Indonesia's digital transformation policies amid increasingly sophisticated cyber threats.

Keywords : *Cyber Defense, Data Breach, Disinformation, Dukcapil*

PENDAHULUAN

Di Zaman digital yang cepat berubah, Indonesia semakin butuh sistem data kependudukan. Ini penting untuk pelayanan publik yang lebih baik. Dukcapil adalah kuncinya. Namun, ketergantungan ini punya risiko siber yang sulit. Ada masalah data bocor besar pada 2023 hingga 2024. Diperkirakan 337 juta data pribadi warga bocor. Kebocoran ini terjadi lewat forum peretas seperti Breach Forums. Isinya termasuk NIK, nama, alamat, dan tanggal lahir. Data akta keluarga juga ikut tersebar. Peristiwa ini merusak percaya masyarakat pada pemerintah. Ini juga membuka celah penipuan siber. Contohnya penipuan berkedok aktivasi IKD. Penipu memakai data yang sudah bocor itu. Selain itu, data bocor menyebar berita bohong. Ini terjadi di media sosial. Hal ini membuat perpecahan sosial makin parah. Stabilitas negara pun terancam. Ancaman hibrida makin besar. Ancaman ini gabungan serangan teknis dan rekayasa informasi. Pemerintah sudah bertindak. BSSN dan Kemendagri melakukan penyelidikan. Format data yang bocor disebut beda dari data resmi. Ini memperjelas perlunya keamanan siber yang giat. Keamanan ini harus melindungi data kependudukan yang penting. Situasi ini membuat Indonesia perlu langkah utuh. Langkah ini harus gabung teknologi enkripsi. Audit rutin juga perlu dilakukan. Perlu juga tingkatkan ilmu digital warga. Semua ini untuk cegah dampak ancaman yang luas.

Strategi pertahanan siber Indonesia dalam menghadapi isu kebocoran data dan disinformasi yang berkaitan dengan Dukcapil tahun 2023-2024 menunjukkan tantangan dalam memperkuat ketahanan nasional di dunia maya. Badan Siber dan Sandi Negara (BSSN) memimpin inisiatif melalui Rencana Aksi Nasional Keamanan Siber (RAN Kamsiber) 2024-2028, yang berfokus pada penguatan infrastruktur informasi yang penting, peningkatan kemandirian dalam kriptografi, serta kerjasama internasional, termasuk pembentukan CSIRT di 264 wilayah untuk merespons insiden. Undang-Undang Perlindungan Data Pribadi (UU PDP) tahun 2022 mengharuskan adanya pelaporan untuk kebocoran data dan adanya sanksi, sedangkan RUU Keamanan dan Ketahanan Siber (RUU KKS) tahun 2025 diusulkan untuk menerapkan prinsip Zero Trust, standar keamanan nasional, serta perlindungan bagi aset strategis seperti data publik. Ancaman disinformasi yang terkait, seperti kampanye negatif yang didasarkan pada data demografis yang bocor, berpotensi menggoyahkan demokrasi dan kebijakan publik, sehingga diperlukan integrasi pertahanan siber aktif dengan peningkatan pemahaman masyarakat mengenai keamanan siber. Analisis kasus ini menyoroti kekurangan dalam sistem yang ada, misalnya kurangnya pengawasan yang merata dan jumlah talenta digital yang terbatas, mengarah pada kebutuhan akan reformasi menyeluruh melalui BSSN sebagai lembaga pemimpin untuk audit forensik yang transparan dan koordinasi antar lembaga. Dengan demikian, penelitian ini bertujuan untuk mengevaluasi efektivitas strategi tersebut dan memberikan rekomendasi yang sesuai bagi pertahanan siber Indonesia di masa mendatang.

LITERATUR REVIEW

1. Fitriani, E., & Trihartono, A. (2021). Cybersecurity and hybrid threats in Indonesia: Challenges for national resilience. *Journal of Asian Security and International Affairs, 8*(2), 175–195. https://doi.org/10.1177/23477970211018436

Penelitian Fitriani dan Trihartono (2021) memberikan gambaran komprehensif mengenai ancaman siber dan *hybrid threats* di Indonesia, terutama terkait tantangan struktural dalam

membangun ketahanan nasional. Fokus utama penelitian tersebut berada pada analisis makro mengenai kapasitas negara, kelemahan institusional, serta fragmentasi tata kelola keamanan siber. Sementara itu, jurnal ini menempatkan analisis pada level yang lebih empiris melalui studi kasus kebocoran data Dukcapil 2023–2024 sebagai contoh konkret dari kegagalan pertahanan siber nasional. Berbeda dengan penelitian Fitriani yang masih bersifat konseptual dan berfokus pada ancaman siber sebelum 2021, penelitian ini mengkaji kebijakan mutakhir seperti RAN Kamsiber 2024–2028, UU PDP 2022, dan RUU KKS 2025, sehingga memberikan kontribusi baru dalam memetakan kesiapan pertahanan siber Indonesia pada konteks ancaman kontemporer. Selain itu, jurnal ini menambahkan dimensi disinformasi sebagai bagian integral dari ancaman hibrida, sesuatu yang tidak dibahas secara mendalam oleh Fitriani. Dengan demikian, penelitian ini tidak hanya memperkuat temuan Fitriani mengenai lemahnya koordinasi dan minimnya sumber daya siber nasional, tetapi juga memperluasnya dengan menunjukkan bagaimana bocornya 337 juta data penduduk dapat memperburuk polarisasi sosial, memicu penipuan identitas, dan mengurangi legitimasi negara, terutama ketika disinformasi memanfaatkan data autentik yang tersebar. Perbandingan ini menunjukkan bahwa jurnal kamu mengisi *gap* signifikan dalam literatur dengan menghadirkan studi kasus terbaru sekaligus mengevaluasi efektivitas kebijakan siber Indonesia dalam menghadapi ancaman teknis dan manipulasi informasi secara bersamaan.

2. Jonathan, L., & Putra, A. (2022). "National Cybersecurity Readiness and Data Protection Challenges in Indonesia." *Journal of Cyber Policy*, 7(3), 245–262.

Studi yang dilakukan oleh Jonathan dan Putra (2022) menekankan rendahnya kesiapan keamanan siber Indonesia dalam melindungi data publik dan mengidentifikasi lemahnya implementasi standar keamanan di instansi pemerintah. Penelitian tersebut berfokus pada analisis struktural mengenai kebijakan keamanan informasi serta hambatan regulasi, namun tidak menyoroti satu insiden besar secara mendalam. Berbeda dengan itu, jurnal ini mengkaji kasus kebocoran data Dukcapil 2023–2024 sebagai contoh konkret kegagalan tata kelola keamanan siber, sehingga memberikan gambaran empiris mengenai bagaimana ketidaksiapan institusional tersebut berujung pada kebocoran 337 juta data warga. Jurnal ini juga memperluas pembahasan Jonathan dan Putra dengan mengintegrasikan analisis disinformasi berbasis data bocor sebagai ancaman lanjutan yang tidak hanya bersifat teknis tetapi juga sosial-politik. Oleh karena itu, jurnal ini tidak hanya mengkonfirmasi temuan mengenai lemahnya kesiapan siber nasional, tetapi juga memberikan kontribusi baru melalui analisis berbasis kasus aktual yang belum dibahas dalam penelitian tahun 2022.

3. Tapsell, R. (2020). Disinformation and the erosion of democratic resilience in Southeast Asia. *Contemporary Southeast Asia*, *42*(1), 1–30.

Penelitian yang dilakukan oleh Tapsell (2020) berfokus pada bagaimana disinformasi melemahkan ketahanan demokrasi di Asia Tenggara melalui manipulasi opini publik dan polarisasi sosial. Meskipun penelitian tersebut menekankan dimensi politik dari disinformasi, ia tidak mengaitkannya dengan serangan siber atau kebocoran data sebagai sumber legitimasi hoaks. Sebaliknya, jurnal ini menempatkan disinformasi sebagai ancaman hibrida yang muncul bersamaan dengan kebocoran data Dukcapil, di mana informasi personal yang bocor digunakan untuk meningkatkan kredibilitas penipuan dan narasi palsu. Jurnal ini secara khusus menunjukkan

bagaimana data autentik memperkuat efektivitas disinformasi, sehingga menghubungkan aspek teknis (serangan siber) dengan aspek sosial-politik (manipulasi informasi). Dengan demikian, penelitian ini memperluas argumen Tapsell dengan memberikan ilustrasi empiris bahwa disinformasi tidak hanya berdampak pada demokrasi, tetapi dapat muncul sebagai akibat dari lemahnya pertahanan siber negara.

PERTANYAAN PENELITIAN

Pertanyaan penelitian merupakan bagian krusial dalam penelitian akademik yang menguraikan isu inti secara spesifik dan terarah, sesuai dengan judul jurnal yang menekankan strategi pertahanan siber Indonesia terhadap kebocoran data dan disinformasi melalui analisis kasus Dukcapil 2023-2024. Pertanyaan ini biasanya mencakup deskripsi fenomena, analisis kelemahan, dan rekomendasi solusi, dengan fokus pada konteks nasional seperti peran BSSN, UU PDP, dan RAN Kamsiber.

1. Bagaimana dinamika ancaman kebocoran data dan disinformasi dalam kasus Dukcapil 2023-2024, termasuk skala (337 juta data bocor), metode serangan (peretasan BreachForums), dan dampaknya terhadap kepercayaan publik serta stabilitas sosial-politik di Indonesia?
2. Sejauh mana efektivitas strategi pertahanan siber Indonesia saat ini, seperti RAN Kamsiber 2024-2028, Peraturan BSSN No. 5/2024, dan RUU KKS 2025, dalam mendeteksi, mencegah, dan menanggulangi kebocoran data massal serta penyebaran disinformasi terkait kasus Dukcapil?
3. Strategi pertahanan siber apa yang dapat dikembangkan secara adaptif oleh Indonesia, termasuk active cyber defense, Zero Trust architecture, dan integrasi CSIRT daerah, untuk menghadapi ancaman hybrid serupa di masa depan berdasarkan analisis kasus Dukcapil?

TEORI PENELITIAN

1. Teori Keamanan dan Pertahanan - Barry Buzan

Barry Buzan memandang keamanan nasional tidak lagi terbatas pada ancaman militer, tetapi mencakup dimensi non-tradisional seperti politik, ekonomi, sosial, lingkungan, dan teknologi. Dalam kerangka ini, keamanan siber masuk sebagai bagian dari sektor keamanan non-tradisional karena menyerang fungsi vital negara tanpa kekuatan bersenjata (Buzan, 1991).

Konsep national security dalam era digital bergeser dari perlindungan wilayah fisik menuju perlindungan sistem informasi strategis. Data kependudukan, jaringan pemerintahan, dan infrastruktur digital menjadi aset nasional yang harus dilindungi setara dengan objek pertahanan konvensional. Serangan siber terhadap data negara berpotensi mengganggu stabilitas politik, pelayanan publik, dan kepercayaan masyarakat. Cyber defense dalam perspektif Buzan menempatkan aktor non-negara sebagai ancaman utama. Kelompok kriminal siber, jaringan hacker internasional, dan penyebar disinformasi berperan signifikan dalam melemahkan keamanan nasional melalui jalur non-militer. Kasus kebocoran data Dukcapil memperkuat argumen ini karena ancaman berasal dari ruang siber dan berdampak langsung pada stabilitas sosial nasional (Buzan, 1991; Interpol, 2023).

2. Teori Pertahanan Siber

Pertahanan siber merujuk pada upaya terintegrasi negara untuk mencegah, mendeteksi, dan merespons ancaman terhadap sistem informasi dan infrastruktur digital strategis. Pertahanan siber tidak hanya bersifat defensif, tetapi juga mencakup langkah proaktif melalui deteksi dini, intelijen ancaman, dan respons cepat terhadap insiden.

BSSN mendefinisikan pertahanan siber sebagai bagian dari ketahanan nasional yang bertujuan melindungi infrastruktur informasi vital, data strategis, dan layanan publik berbasis digital. Dalam praktiknya, pertahanan siber mencakup pengamanan teknis, tata kelola kebijakan, koordinasi antar lembaga, serta kesiapan sumber daya manusia (BSSN, 2024).

Pendekatan modern pertahanan siber menekankan penerapan Zero Trust architecture, yaitu prinsip tidak ada entitas yang dipercaya secara otomatis, baik dari dalam maupun luar sistem. Setiap akses harus diverifikasi secara ketat. Pendekatan ini relevan dengan kasus Dukcapil karena kebocoran data diduga berkaitan dengan kelemahan pengendalian akses dan pengawasan internal (Shafira et al., 2024).

3. Teori Disinformasi - Wardle & Derakhshan

Wardle dan Derakhshan (2017) mengembangkan kerangka teoretis yang dikenal sebagai *Information Disorder Framework,* yaitu teori yang menjelaskan bagaimana gangguan informasi bekerja dalam ruang digital. Mereka memetakan tiga bentuk utama gangguan informasi: *misinformation,* yaitu informasi yang salah tetapi disebarkan tanpa niat jahat; *disinformation*, yaitu informasi yang salah dan sengaja diproduksi untuk merusak, menipu, atau memanipulasi publik; dan *malinformation*, yaitu informasi yang benar tetapi dibocorkan atau digunakan untuk tujuan merugikan. Kerangka ini menekankan bahwa disinformasi bukan sekadar penyebaran informasi palsu, tetapi merupakan tindakan strategis yang diproduksi oleh aktor tertentu dengan motivasi politik, ekonomi, atau ideologis.

Wardle dan Derakhshan juga menekankan bahwa disinformasi bekerja melalui tiga elemen kunci: aktor, konten, dan distribusi. Aktor dapat berupa individu, kelompok politik, negara asing, atau organisasi kriminal yang memiliki kepentingan tertentu. Konten disinformasi biasanya dirancang agar emosional, provokatif, atau tampil seperti informasi resmi sehingga mudah dipercaya. Distribusi disinformasi dipercepat melalui media sosial, bot otomatis, algoritma platform digital, dan ruang percakapan tertutup, sehingga menghasilkan penyebaran cepat dan sulit dikendalikan. Teori ini juga menjelaskan bahwa disinformasi memiliki dampak signifikan terhadap stabilitas politik dan keamanan nasional karena dapat mengikis kepercayaan publik, menciptakan polarisasi sosial, serta mengganggu legitimasi institusi negara.

Dalam konteks penelitian tentang kebocoran data dan pertahanan siber, teori Wardle dan Derakhshan menjelaskan bahwa disinformasi sering memanfaatkan data asli untuk meningkatkan kredibilitas informasi palsu. Hal ini relevan dengan kasus kebocoran data Dukcapil 2023–2024, di mana informasi personal yang bocor digunakan dalam penipuan, phishing, dan hoaks terkait aktivasi layanan digital. Dengan demikian, teori ini memberikan landasan kuat untuk menganalisis bagaimana disinformasi muncul sebagai ancaman lanjutan setelah serangan siber, serta bagaimana dinamika informasi tersebut dapat memperburuk kerentanan masyarakat dan melemahkan keamanan nasional.

METODOLOGI

Penelitian ini menggunakan pendekatan kualitatif deskriptif-analitis karena berupaya memahami secara mendalam proses, strategi, serta dinamika pertahanan siber Indonesia dalam menghadapi ancaman kebocoran data dan disinformasi, khususnya pada kasus kebocoran data Dukcapil tahun 2023–2024. Pendekatan kualitatif memungkinkan peneliti menggali informasi melalui analisis dokumen, peraturan, laporan teknis, pemberitaan, serta wawancara dengan pihak terkait untuk mendapatkan pemahaman komprehensif mengenai bagaimana pemerintah merespons serta mengelola risiko siber. Analisis data dalam penelitian ini dilakukan dengan menggunakan pendekatan kualitatif deskriptif-analitis yang berfokus pada pengolahan dan penafsiran data dokumenter yang telah dikumpulkan dari berbagai sumber. Analisis dilakukan secara bertahap mengikuti model analisis kualitatif menurut Miles, Huberman, dan Saldaña (2014) dengan tiga proses utama: reduksi data, penyajian data, dan penarikan kesimpulan, serta prinsip *pattern matching* dan *explanation building* dari Yin (2018) sebagai elemen khas studi kasus.

Deskriptif-analitis digunakan karena penelitian tidak hanya memaparkan fakta dan fenomena secara rinci, tetapi juga menganalisis hubungan antara faktor penyebab, bentuk ancaman, respons institusi, serta efektivitas kebijakan yang diterapkan. Melalui pendekatan ini, penelitian berfokus pada pemaknaan, interpretasi, serta evaluasi strategi pertahanan siber, sehingga menghasilkan gambaran yang mendalam mengenai kesiapan Indonesia dalam menghadapi eskalasi ancaman kebocoran data dan disinformasi yang semakin kompleks di era digital.

HASIL DAN PEMBAHASAN

1. Peta Ancaman Siber Indonesia

Selain kebocoran data Dukcapil, peta ancaman siber Indonesia juga semakin sulit karena meningkatnya aktivitas *ransomware*, *phishing*, dan serangan terhadap infrastruktur informasi vital (IIV). BSSN pada laporan tahunan 2024 mencatat lebih dari 370 juta anomali siber yang terdeteksi sepanjang tahun, dengan mayoritas serangan menyasar sektor pemerintahan, layanan publik, dan energi (BSSN, 2024). Lonjakan ini terjadi seiring dengan meningkatnya digitalisasi layanan, yang belum diimbangi dengan peningkatan kemampuan pertahanan siber yang memadai. Serangan *ransomware* seperti yang terjadi pada Bank Syariah Indonesia (BSI) pada 2023 juga menjadi bukti bahwa ancaman tidak hanya bersifat pencurian data, tetapi sudah berkembang menjadi sabotase layanan publik yang dapat mengganggu stabilitas ekonomi dan kepercayaan masyarakat.

Ancaman siber di Indonesia juga diperburuk oleh keberadaan *threat actor* internasional yang memanfaatkan kerentanan sistem nasional. Menurut laporan Cybersecurity and Infrastructure Security Agency (CISA) dan Interpol, Asia Tenggara termasuk Indonesia menjadi salah satu kawasan paling rentan karena lemahnya regulasi keamanan data dan minimnya investasi pada *cyber workforce* (Interpol, 2023). Pada kasus Dukcapil, pola serangan ini menunjukkan potensi keterlibatan *organized cybercrime* yang menggabungkan antara teknik eksploitasi database dengan aktivitas penjualan data pada forum gelap, menunjukkan bahwa ancaman tidak lagi berasal dari individu, tetapi kelompok terorganisir dengan kemampuan teknis tinggi. Hal ini dapat mengonfirmasi argumen Buzan (1991) bahwa aktor non-negara kini memainkan peran semakin signifikan dalam mengancam keamanan nasional melalui jalur non-militer.

Selain aspek teknis, psikologis dan sosial dari ancaman siber juga menjadi bagian penting dari peta ancaman nasional. Setelah kebocoran data Dukcapil beredar, ruang digital Indonesia

dibanjiri hoaks terkait identitas, penipuan berbasis data asli, serta kampanye yang menargetkan kelompok tertentu berdasarkan data kependudukan. Wardle & Derakhshan (2017) menyatakan bahwa disinformasi modern menjadi lebih berbahaya ketika dikombinasikan dengan data nyata yang bocor karena hoaks menjadi lebih meyakinkan dan sulit dibantah. Dalam konteks Indonesia, hal ini tercermin dari meningkatnya penipuan digital pasca-insiden, seperti penipuan aktivasi IKD, undangan palsu, dan manipulasi data keluarga yang memanfaatkan kredibilitas informasi bocor. Dengan demikian, peta ancaman siber Indonesia harus dipahami bukan hanya sekedar persoalan teknologi, tetapi ancaman multidimensi yang menembus keamanan informasi, psikologi sosial, ekonomi digital, hingga legitimasi negara.

Hasil penelitian menunjukkan ancaman siber di Indonesia mengalami eskalasi signifikan seiring percepatan transformasi digital sektor publik. Data BSSN mencatat ratusan juta anomali trafik siber setiap tahun, dengan tren dominan berupa phishing, malware, ransomware, serta kebocoran data berskala besar. Pola ini memperlihatkan pergeseran ancaman dari sekadar gangguan teknis menuju ancaman strategis yang berimplikasi langsung pada stabilitas nasional. Sektor pemerintah menjadi target utama karena mengelola data bernilai tinggi, terutama data kependudukan, fiskal, dan layanan publik digital. Sistem yang terhubung lintas instansi, penggunaan pihak ketiga, serta standar keamanan yang tidak seragam meningkatkan permukaan serangan. Kebocoran data Dukcapil memperlihatkan kerentanan struktural dalam pengelolaan database nasional yang seharusnya termasuk infrastruktur informasi vital. Ancaman kebocoran data juga beririsan dengan serangan espionase dan kejahatan terorganisir. Data kependudukan memiliki nilai strategis untuk pemetaan demografis, rekayasa sosial, dan operasi intelijen. Dengan demikian, ancaman siber di Indonesia bersifat multidimensi, meliputi aspek teknis, ekonomi, sosial, hingga pertahanan negara.

2. Posisi dan Strategi Pertahanan Siber Nasional

Meski Indonesia telah memiliki kerangka kebijakan yang cukup komprehensif, tantangan terbesar terletak pada implementasi keamanan siber yang belum bisa terintegrasi secara nasional. RAN Kamsiber 2024–2028 menekankan penguatan infrastruktur informasi vital, tetapi pelaksanaannya masih terbatas oleh disparitas kapasitas antarinstansi dan pemerintah daerah (BSSN, 2024). Banyak lembaga pemerintah terutama di daerah belum memiliki standar keamanan informasi yang memadai, seperti manajemen kerentanan, audit digital rutin, atau sistem pemantauan ancaman berbasis AI. Ketergantungan pada metode administratif dan manual dalam mendeteksi dan menangani ancaman membuat Indonesia tertinggal dibanding negara-negara lain yang telah lebih dahulu mengadopsi *active cyber defense*. Hal ini memperlihatkan bahwa meskipun kebijakan sudah tersedia, kesiapan kelembagaan dan infrastruktur teknis belum cukup kuat untuk memberikan perlindungan menyeluruh terhadap ancaman besar seperti kebocoran data Dukcapil.

Mendalami lebih dalam, pembangunan Computer Security Incident Response Team (CSIRT) di 264 daerah merupakan langkah strategis untuk memperkuat respons insiden pada tingkat lokal. Namun, dari sisi kualitas, sebagian besar CSIRT menghadapi tantangan berupa kurangnya tenaga ahli keamanan siber, minimnya anggaran operasional, serta belum tersedianya fasilitas *threat intelligence* yang mumupuni. Interpol (2023) dalam laporannya menekankan bahwa Asia Tenggara, termasuk Indonesia, mengalami kekurangan talenta siber yang signifikan, sehingga upaya respons insiden seringkali hanya berfokus pada pemulihan dasar, bukan analisis forensik mendalam atau mitigasi jangka panjang. Kondisi ini menyebabkan koordinasi antar-

CSIRT dan pusat komando nasional belum berjalan optimal. Ketergantungan pada vendor luar negeri untuk penanganan teknis tertentu juga menimbulkan risiko tambahan, terutama terkait kedaulatan data dan keamanan infrastruktur strategis.

Di sisi regulasi, UU Perlindungan Data Pribadi (UU PDP) 2022 sebenarnya telah memberikan landasan hukum yang kuat melalui kewajiban pelaporan insiden dan penerapan sanksi administratif hingga pidana bagi pengendali data yang lalai. Namun, tanpa adanya Otoritas Perlindungan Data Independen yang berfungsi sebagai regulator teknis, pengawas, dan penegak hukum, aturan ini belum dapat diimplementasikan secara efektif (Kominfo, 2023). Selain itu, regulasi keamanan seperti Peraturan BSSN No. 5/2024 yang mengatur penanganan insiden siber juga belum memiliki kekuatan yang cukup untuk memaksa seluruh instansi menerapkan standar keamanan nasional yang sama. Hal ini menyebabkan fragmentasi tata kelola keamanan informasi, di mana beberapa lembaga telah maju dalam adopsi Zero Trust, sementara yang lain masih bergantung pada sistem lama yang rentan. Maka, untuk membangun pertahanan siber nasional yang kokoh, Indonesia perlu memperkuat penegakan regulasi, menstandardisasi penerapan keamanan, dan memastikan bahwa lembaga teknis seperti BSSN memiliki kewenangan operasional yang lebih besar untuk mengkoordinasikan seluruh instansi.

Analisis per lembaga menunjukkan pertahanan siber nasional telah memiliki pembagian peran formal, namun belum sepenuhnya terintegrasi secara operasional. BSSN berperan sebagai operator pertahanan siber dengan mandat pengamanan infrastruktur informasi vital, koordinasi CSIRT, serta penyusunan kebijakan teknis. Namun, kapasitas BSSN masih terbatas pada fungsi koordinatif, dengan kewenangan yang belum cukup kuat untuk memaksa kepatuhan lintas instansi. Kementerian Pertahanan memposisikan siber sebagai bagian dari postur pertahanan negara, tetapi fokus masih dominan pada doktrin dan kebijakan makro. Integrasi siber ke dalam sistem pertahanan militer belum sepenuhnya terhubung dengan insiden sipil seperti kebocoran data kependudukan. BIN berfungsi dalam intelijen siber, khususnya deteksi dini ancaman strategis dan aktor asing. Keterbatasan berbagi intelijen lintas lembaga menyebabkan informasi ancaman sering terfragmentasi. Kominfo memegang peran tata kelola data dan regulasi ruang digital, termasuk perlindungan data pribadi. Namun, lemahnya pengawasan teknis dan belum terbentuknya otoritas perlindungan data independen mengurangi efektivitas peran ini. Polri berfokus pada penegakan hukum siber. Proses penindakan sering bersifat reaktif dan menghadapi tantangan pembuktian teknis lintas yurisdiksi. Secara keseluruhan, strategi pertahanan siber nasional masih berjalan sektoral dan belum membentuk satu sistem pertahanan terpadu.

3. Studi Kasus Kebocoran Data Dukcapil 2023–2024

Kasus kebocoran data Dukcapil 2023–2024 semakin menunjukkan bahwa tata kelola keamanan data kependudukan Indonesia belum berada pada tingkat yang memadai untuk menghadapi serangan siber berskala besar. Kebocoran data 337 juta penduduk bukan hanya mencerminkan kerentanan teknis, tetapi juga lemahnya manajemen risiko, kurangnya segmentasi data, serta minimnya deteksi dini terhadap aktivitas mencurigakan di server pemerintah (CNN Indonesia, 2023). Analisis forensik BSSN mengindikasikan bahwa kebocoran terjadi bukan dalam bentuk *full database*, melainkan kompilasi data yang sangat mirip dengan data resmi, sehingga kemungkinan berasal dari celah akses atau rekayasa pihak ketiga (BSSN, 2024). Hal ini memperlihatkan bahwa risiko tidak hanya muncul dari serangan eksternal, tetapi juga dari pihak internal atau mitra yang memiliki hak akses tetapi tanpa pengawasan ketat fenomena yang sering

disebut sebagai *insider threat*. Masalah mendasar ini menunjukkan bahwa penguatan keamanan harus mencakup audit akses berkala dan sistem pemantauan real-time berbasis Zero Trust.

Selain itu, pemanfaatan data bocor untuk kegiatan kriminal seperti penipuan identitas, rekayasa sosial, dan penyalahgunaan layanan digital menunjukkan bahwa dampak insiden tidak berhenti pada hilangnya kerahasiaan data, tetapi juga mengancam keamanan ekonomi dan kehidupan sosial masyarakat. Maraknya modus aktivasi IKD palsu dan penawaran layanan yang memanfaatkan data autentik menjadi bukti bahwa kebocoran data memberikan keuntungan besar bagi pelaku kejahatan siber yang menggabungkan teknik teknis dengan teknik manipulatif terhadap psikologi korban. Situasi ini sejalan dengan temuan Interpol (2023) bahwa Asia Tenggara mengalami lonjakan kejahatan berbasis identitas sebagai konsekuensi langsung dari lemahnya perlindungan data. Dalam konteks Dukcapil, kebocoran data menyebabkan meningkatnya laporan penipuan daring, hilangnya privasi, serta beban keamanan tambahan bagi masyarakat yang pada dasarnya tidak memiliki kemampuan teknis untuk memahami risiko lanjutan.

Kronologi insiden menunjukkan data Dukcapil beredar di forum peretas internasional sejak 2023 dan kembali mencuat pada 2024 dengan klaim skala ratusan juta data. Data yang tersebar mencakup NIK, nama lengkap, alamat, tanggal lahir, serta data keluarga, yang memiliki tingkat sensitivitas tinggi. Secara teknis, dugaan penyebab mengarah pada kelemahan pengelolaan akses, pemanfaatan API tanpa pengamanan memadai, kredensial yang bocor, serta keterkaitan dengan Pusat Data Nasional. Temuan ini mengindikasikan kegagalan prinsip least privilege dan lemahnya pemantauan akses. Respons pemerintah meliputi klarifikasi publik, investigasi oleh BSSN dan Kemendagri, serta penegasan bahwa data tidak identik dengan database resmi. Namun, respons ini dinilai lambat dan kurang transparan, sehingga tidak sepenuhnya meredam keresahan publik. Dampak terhadap pertahanan nasional terlihat dari meningkatnya penipuan berbasis identitas, menurunnya kepercayaan publik terhadap negara, serta terbukanya peluang eksploitasi data untuk kepentingan politik dan intelijen asing. Kasus ini menegaskan bahwa kebocoran data kependudukan bukan sekadar isu administratif, tetapi ancaman strategis.

KESIMPULAN

Ancaman kebocoran data merupakan persoalan serius karena dapat merusak ketahanan dan pertahanan nasional. Ketika data strategis warga atau institusi bocor, negara berpotensi kehilangan keunggulan informasi, menghadapi gangguan layanan publik, dan menjadi lebih rentan terhadap pemerasan, sabotase, maupun operasi intelijen pihak luar. Dampaknya bukan hanya teknis, tetapi juga politis dan sosial, karena menurunkan kepercayaan publik terhadap kemampuan negara melindungi warganya.

Strategi pertahanan siber yang berjalan saat ini masih menyisakan celah pada level implementasi. Meski kebijakan dan kerangka kerja sudah ada, penerapan di lapangan sering tidak seragam antarinstansi, kurang diawasi, serta belum didukung sumber daya manusia dan anggaran yang memadai. Akibatnya, standar keamanan hanya kuat di atas kertas, sementara sistem-sistem kritikal tetap rentan karena tata kelola, prosedur respons insiden, dan pengujian keamanan belum berfungsi konsisten.

Kasus kebocoran data Dukcapil menjadi contoh nyata bahwa reformasi tata kelola data adalah kebutuhan mendesak. Kejadian tersebut menunjukkan lemahnya pengendalian akses, minimnya audit, serta rendahnya disiplin keamanan dalam pengelolaan data berisiko tinggi. Dengan skala dan sensitivitas data kependudukan, kebocoran semacam ini dapat menimbulkan

efek berantai mulai dari penipuan identitas hingga ancaman keamanan nasional sehingga pembenahan sistemik perlu dilakukan, bukan sekadar penanganan insidental.

Rekomendasi

Penguatan national cyber defense perlu ditempatkan sebagai prioritas utama melalui peningkatan kapabilitas deteksi dini, pencegahan, dan respons insiden pada infrastruktur kritikal. Hal ini mencakup modernisasi teknologi keamanan, integrasi pusat pemantauan ancaman nasional, serta penyusunan doktrin pertahanan siber yang jelas agar setiap instansi memiliki arah tindakan yang sama dalam menghadapi serangan siber yang semakin kompleks dan terkoordinasi.

Penerapan wajib standar ISO/IEC 27001 di seluruh instansi pemerintah harus dilakukan untuk memastikan adanya sistem manajemen keamanan informasi yang terukur dan konsisten. Standar ini bukan hanya soal dokumentasi, tetapi tentang siklus pengelolaan risiko, kontrol keamanan, evaluasi berkala, serta perbaikan berkelanjutan. Dengan kewajiban ini, gap kualitas keamanan antarinstansi dapat dipersempit dan kepatuhan terhadap praktik terbaik internasional menjadi lebih terjamin.

Pembentukan Cyber Joint Command dibutuhkan untuk memperkuat koordinasi lintas lembaga dalam satu struktur komando yang responsif. Model ini memungkinkan pertukaran intelijen ancaman secara real time, orkestrasi respons insiden berskala nasional, serta penegasan peran dan tanggung jawab saat terjadi serangan pada sektor strategis. Tanpa komando terpadu, penanganan ancaman akan cenderung terfragmentasi dan lambat.

Percepatan implementasi UU Perlindungan Data Pribadi (UU PDP) harus dipastikan melalui aturan turunan yang operasional, pembentukan otoritas pengawas yang efektif, serta mekanisme sanksi yang tegas. Implementasi cepat akan mendorong instansi pemerintah dan pihak terkait lain lebih disiplin dalam pemrosesan data, memperjelas kewajiban perlindungan, serta memberi landasan hukum kuat untuk pencegahan dan penindakan kebocoran data.

Peningkatan kapasitas personel dan audit keamanan perlu dijalankan secara berkesinambungan agar pertahanan siber tidak hanya bergantung pada teknologi. Pelatihan teknis, sertifikasi, simulasi serangan, dan peningkatan literasi keamanan bagi seluruh pegawai harus diiringi audit rutin dan penetration testing independen. Dengan begitu, kelemahan dapat ditemukan lebih awal dan budaya keamanan terbentuk di seluruh organisasi.

Penguatan mekanisme kontra-disinformasi nasional juga krusial karena ancaman siber sering beriringan dengan operasi informasi. Negara perlu membangun sistem deteksi, klarifikasi cepat, dan edukasi publik yang terkoordinasi untuk meredam hoaks yang dapat memicu instabilitas sosial atau melemahkan legitimasi institusi. Upaya ini harus melibatkan kolaborasi pemerintah, platform digital, media, dan masyarakat sipil agar responnya cepat sekaligus kredibel.

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara. (2024). *Rencana Aksi Nasional Keamanan Siber (RAN Kamsiber) 2024–2028*. BSSN RI.

Badan Siber dan Sandi Negara. (2023). *Laporan Tahunan Keamanan Siber Indonesia 2023*. BSSN RI.

Badan Siber dan Sandi Negara. (2024). *Evaluasi insiden siber nasional: Laporan tahunan 2024.* BSSN RI.

Badan Siber dan Sandi Negara. (2024). *Laporan Tahunan Keamanan Siber Nasional 2024*. BSSN RI.

Buzan, B. (1991). *People, States & Fear: An Agenda for International Security Studies in the Post–Cold War Era*. Harvester Wheatsheaf.

CNN Indonesia. (2023, July 18). *Data Dukcapil diduga bocor 337 juta identitas penduduk tersebar di forum hacker.* CNN Indonesia.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Cybersecurity and Infrastructure Security Agency. (2022). *CISA Cybersecurity Advisory: Threats to National Data Infrastructure*. U.S. Department of Homeland Security.

Fitriani, A., & Trihartono, A. (2021). Cybersecurity and hybrid threats in Indonesia: Challenges for national resilience. *Journal of Asian Security and International Affairs, 8*(2), 175–195.

Interpol. (2023). *ASEAN Cyberthreat Landscape 2023: Regional Cybercrime Assessment*. INTERPOL Cybercrime Directorate.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Laporan penanganan insiden kebocoran data Dukcapil 2023*. Kominfo RI.

Kementerian Komunikasi dan Informatika RI. (2023). *Siaran pers: Penjelasan dugaan kebocoran data Dukcapil.* Kominfo RI.

Nurhidayat, D., & Prasetyo, A. (2022). Disinformation and digital vulnerability in Indonesia's online space. *Jurnal Komunikasi Indonesia, 11*(1), 44–58.

Nurhidayat, R., dan Prasetyo, A. 2022. Disinformasi sebagai ancaman keamanan nasional non militer. Jurnal Keamanan Nasional, 8(2), 145–160.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*.

Republik Indonesia. (2025). *Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS)*. DPR RI.

Shafira, N., Putra, R. A., dan Lestari, D. 2024. Pertahanan siber dan kebocoran data kependudukan di Indonesia. Jurnal Pertahanan dan Keamanan Siber, 3(1), 22–38.

Stake, R. E. (1995). *The art of case study research.* SAGE Publications.

Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Council of Europe.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.