JRAM (Jurnal Riset Akuntansi Multiparadigma)

ISSN: 2599-1469 ‖ https://jurnal.uisu.ac.id/index.php/JRAM

Eksplorasi Implementasi Kebijakan Pembentukan *Computer Security Incident Response Team* (CSIRT) Di Kementerian Perdagangan: Sebuah Studi Kualitatif

Ana Najiyya[1]*, Stepani Sisca Wulandari[2]

Magister Akuntansi, Sekolah Pasca Sarjana, Perbanas Institute, Jakarta Selatan, Indonesia

***Corresponding author*:** ana.najiyya@gmail.com

ARTICLE INFO

Article history
Received :
Accepted :
Published :

Kata Kunci:
Kejahatan;
Siber;
CSIRT;
Kementerian Perdagangan;
BSSN.

A B S T R A K

Computer Security Incident Response Team (CSIRT) Kementerian Perdagangan adalah tim tanggap insiden siber yang dibentuk berdasarkan Peraturan BSSN No. 10/2020 tentang Tim Tanggap Insiden Siber. Tujuan dibentuknya tim ini yaitu untuk dapat memastikan bahwa sistem elektronik dan layanan publik telah berjalan dengan baik dan aman dari serangan siber. Sehingga penelitian ini bertujuan untuk mengkaji pelaksanaan kebijakan BSSN di Kementerian Perdagangan terkait pembentukan CSIRT berdasarkan Peraturan BSSN No. 10 Tahun 2020 berdasarkan implementasinya dengan menggunakan metode kualitatif melalui pendekatan deskriptif eksploratif. Hasil penelitian menunjukkan bahwa pelaksanaan CSIRT saat ini belum optimal dan tersendat oleh beberapa kendala, seperti struktur pengambilan keputusan yang birokratis, keterbatasan sumber daya manusia, dan lemahnya kewenangan unit PDSI. Untuk mengatasi kendala-kendala tersebut, diperlukan peningkatan struktur pengambilan keputusan, peningkatan jumlah dan kompetensi SDM, serta penerapan teknologi big data yang lebih efektif dan efisien dalam mengelola keamanan siber.

Keyword:
Crime;
Cyber;
CSIRTs;
Ministry of Trade;
BSSN

A B S T R A C T

The Ministry of Trade's Computer Security Incident Response Team (CSIRT) is a cyber incident response team formed under BSSN Regulation No. 10 of 2020 concerning the Cyber Incident Response Team. The purpose of forming this team is to ensure that electronic systems and public services are running correctly and are safe from cyber-attacks. This study aims to examine the implementation of the BSSN policy at the Ministry of Trade regarding establishing the CSIRT based on BSSN Regulation No. 10 of 2020 based on its implementation using a qualitative method through a descriptive exploratory approach. The study results show that the current implementation of CSIRT is not optimal and is hampered by several obstacles, such as the bureaucratic decision-making structure, limited human resources, and the weak capacity of the PDSI unit. To overcome these obstacles, it is necessary to improve the decision-making structure, increase the number and competence of human resources, and apply big data technology that is more effective and efficient in managing cyber security.

PENDAHULUAN

Perkembangan pesat di bidang teknologi informasi dan komunikasi, serta big data, telah menjadikan keamanan siber sebagai masalah strategis di banyak negara, termasuk Indonesia. Hal ini terlihat pada Pidato Kenegaraan Sidang DPR DPD RI 2019, di mana Presiden Joko Widodo menekankan pentingnya kesadaran akan ancaman kejahatan siber, seperti pencurian data, bagi Negara (Parulian, Pratiwi, & Cahya Yustina, 2021). Mengingat data merupakan jenis kekayaan baru di Indonesia, negara ini perlu mempersiapkan diri untuk menghadapi perang cyber demi menjaga pertahanan keamanannya (Babys, 2021). Sayangnya, berdasarkan data National Cyber Security Index (NCSI) pada tahun 2022, Indonesia hanya memperoleh poin 38,96 dari 100, menempatkan negara ini pada peringkat ketiga terendah dalam keamanan siber di antara negara-negara Group of Twenty (G20)(Aji, 2023; Chotimah, 2019).Pada periode 1 Januari hingga 19 Maret 2021, data center Kementerian Perdagangan mengalami lebih dari 500.000 percobaan serangan cyber sebelum pembentukan Computer Security Incident Response Team (CSIRT), menurut data perangkat keamanan Kementerian Perdagangan (Amanowicz, 2021; Rai, Heryadi, & Kamaluddin N., 2022). Kementerian Perdagangan memiliki banyak data dan aplikasi pelayanan publik yang terkait dengan sistem perizinan dalam dan luar negeri, perlindungan konsumen, serta perdagangan berjangka komoditi, yang tentu saja memiliki risiko jika terkena serangan cyber (Annef, 2021). Dalam konteks ini, big data berperan penting dalam akuntansi, seperti analisis tren pasar, peramalan, manajemen keuangan, dan pengambilan keputusan bisnis, sehingga keamanan data menjadi sangat penting bagi sektor ini (Bhardwaj & Sapra, 2021; Wulandari, 2023).

Serangan ini dapat berakibat pada penurunan kredibilitas Kementerian Perdagangan, gangguan pada sistem operasional pelayanan publik, serta kerugian finansial bagi pelaku usaha yang berdampak pada perekonomian nasional (Bhardwaj & Sapra, 2021; Indramawan, Handayanto, & Djajanti, 2021) CSIRT Kementerian Perdagangan merupakan tim tanggap insiden siber yang dibentuk berdasarkan Peraturan BSSN No. 10 Tahun 2020 tentang Tim Tanggap Insiden Siber (Patent No. 10, 2020; Kementerian Perdagangan Republik Indonesia, 2021). Pembentukan tim CSIRT Kementerian Perdagangan juga merupakan tindak lanjut dari Surat Kepala Badan Siber dan Sandi Negara (BSSN) Nomor T.61/BSSN/D3/PP.01.07/03/2021 tentang Penunjukan Instansi Pemerintah dalam Program *Computer Security Incident Respond* (CSIRT) Tahun 2021 (Patent No. 6, 2021). Pembentukan CSIRT pada instansi Kementerian Perdagangan sejalan dengan penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) yang diatur dalam Peraturan Presiden No. 95 Tahun 2018 tentang SPBE (Pemerintah Pusat, 2018). Dalam peraturan tersebut, menyatakan bagian unsur keamanan SPBE yaitu meliputi penjaminan kerahasiaan, kebutuhan dan ketersediaan data dan informasi, yang mencakup pemeliharaan dan analisis big data khususnya dalam bidang akuntansi. Peran CSIRT di sini adalah untuk memonitor dan memulihkan sistem apabila terjadi insiden keamanan siber.

Sejak awal tahun 2021, penilaian tingkat kematangan penanganan insiden telah dimulai oleh CSIRT Kementerian Perdagangan melalui pendampingan, hingga akhirnya diresmikan pada 27 Mei 2021 yang ditetapkan melalui SK Sekretaris Jenderal Kementerian Perdagangan Nomor 456 Tahun 2021 perihal Pembentukan Kementerian Perdagangan Computer Security Incident Response Team (Kementerian Perdagangan Republik Indonesia, 2021). Pada artikel ini memodifikasi penelitian sebelumnya yang dilakukan oleh Prabaswari et al., (2022) yang berjudul Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. Oleh karena itu tujuan dari penelitian ini adalah untuk mengkaji pelaksanaan kebijakan BSSN di Kementerian Perdagangan terkait pembentukan CSIRT berdasarkan Peraturan BSSN No. 10 Tahun 2020 berdasarkan implementasinya, serta menyoroti pentingnya keamanan big data dalam bidang akuntansi.

KAJIAN LITERATUR

Keamanan Siber dan Big Data

Keamanan siber merupakan isu yang penting dalam era digital ini, khususnya dengan adanya perkembangan teknologi big data yang digunakan berbagai sektor seperti pemerintahan, bisnis, perkotaan, dan akuntansi (Zhang & Dong, 2023). Seiring dengan kemajuan teknologi, banyak organisasi mulai menggunakan Big Data untuk mengumpulkan, menganalisis, dan memanfaatkan informasi dalam jumlah besar dari berbagai sumber data, dengan tujuan untuk meningkatkan efisiensi operasional, mendukung pengambilan keputusan, dan menciptakan strategi yang lebih efektif. Namun, peningkatan penggunaan Big Data dalam akuntansi juga menimbulkan tantangan di bidang keamanan siber. Informasi akuntansi yang sangat konfidensial, seperti data keuangan, transaksi, dan informasi pelanggan, menjadi target potensial bagi pelaku serangan siber (Chałubińska-Jentkiewicz, Radoniewicz, & Zieliński, 2022). Oleh karena itu, penting bagi organisasi dan praktisi akuntansi untuk mengembangkan dan mengimplementasikan langkah-langkah keamanan yang efektif dalam rangka melindungi integritas, kerahasiaan, dan ketersediaan data akuntansi yang sangat penting tersebut. Implementasi CSIRT (*Computer Security Incident Response Team*) dalam organisasi, misalnya, dapat

membantu memberikan dukungan, koordinasi, dan kebijakan dalam menghadapi insiden keamanan siber, sehingga meminimalkan risiko kerugian dan dampak negatif pada bisnis serta menjaga kepercayaan pihak-pihak yang relevan (Berardi, Tippenhauer, Melis, Prandini, & Callegati, 2023). Hal ini menjadi sebab mengapa keamanan siber menjadi tanggung jawab bersama antara pemerintah dan pemangku kepentingan dalam menjaga integritas, kerahasiaan, dan ketersediaan data. Pada bidang akuntansi, data berkualitas, cepat, dan akurat sangat penting karena dapat mempengaruhi pengambilan keputusan bisnis yang berkualitas (Alzubaidi et al., 2023). Big data memungkinkan analisis tren pasar dengan lebih efisien, dimana analisis ini sangat bergantung pada keamanan data yang diolah. CSIRT, melalui implementasi praktik terbaik dalam keamanan siber, dapat meningkatkan kualitas big data dan menjaga informasi yang menjadi aset penting dari banyak organisasi, termasuk di sektor akuntansi. Oleh karena itu, diperlukan kerjasama antara sektor akuntansi dan keamanan siber dalam menciptakan sinergi yang saling menguntungkan.

Implementasi CSIRT di Kementerian Perdagangan

Implementasi *Computer Security Incident Response Team* (CSIRT) di Kementerian Perdagangan memiliki peran yang cukup signifikan, terutama dalam bidang akuntansi dan keuangan. CSIRT bertindak sebagai garda terdepan dalam menghadapi ancaman siber yang berpotensi merusak integritas data keuangan dan mengakibatkan dampak negatif bagi kelangsungan operasional Kementerian Perdagangan (Ubowska & Królikowski, 2022). Melalui penerapan mekanisme CSIRT, pihak kementerian bisa memastikan keandalan dan keberlanjutan sistem informasi akuntansinya, sehingga dapat melindungi kepentingan publik dan mengamankan data sensitif terkait transaksi keuangan pemerintah. Dalam bidang akuntansi, implementasi CSIRT meliputi pelacakan dan investigasi potensi serangan siber yang mencakup penipuan dan pencurian data, serta melindungi sistem akuntansi kementerian dari ancaman eksternal dan internal (Amanowicz, 2021). Hal ini melibatkan kolaborasi antara pemangku kepentingan internal dan eksternal seperti auditor, ahli sistem informasi, dan ahli keamanan siber, serta mendukung pengembangan kapasitas personel yang merupakan bagian dari CSIRT. Selain itu, tim CSIRT juga bertanggung jawab untuk mengembangkan skenario rencana pemulihan data, kebijakan, dan prosedur respon keamanan, serta menguji ketahanan dan kesiapan infrastruktur TI kementerian dalam menghadapi insiden keamanan. Dengan melalui serangkaian langkah ini, implementasi CSIRT di Kementerian Perdagangan menjadi bagian penting dalam menjaga integritas sistem akuntansi dan keuangan pemerintah.

METODOLOGI PENELITIAN

Penelitian ini bertujuan untuk mengkaji pelaksanaan kebijakan BSSN di Kementerian Perdagangan dengan menggunakan metode kualitatif melalui pendekatan deskriptif eksploratif. Data yang digunakan dalam penelitian ini merupakan data primer yang diperoleh melalui wawancara terstruktur, yang memungkinkan peneliti untuk memahami bagaimana kebijakan tersebut diimplementasikan dan efektivitasnya dalam menjaga keamanan sistem informasi di Kementerian Perdagangan. Sebagai peneliti, akan menggali informasi lebih dalam mengenai CSIRT dan bagaimana implementasi kebijakan ini telah memberikan dampak pada peningkatan keamanan dan mitigasi risiko terkait dengan insiden keamanan *cyber*.

HASIL DAN PEMBAHASAN

Hasil penelitian ditulis dalam bentuk paragraf mengalir yang ditulis dengan sistematis, analisis yang kritis, dan informatif. Penggunaan tabel, gambar dsb hanya sebagai pendukung yang memperjelas pembahasan dan dibatasi hanya pada pendukung yang benar-benar substantial, misalnya tabel hasil pengujian statistik, gambar hasil pengujian model dsb. Pembahasan hasil bersifat argumentatif menyangkut relevansi antara hasil, teori, penelitian terdahulu dan fakta empiris yang ditemukan, serta menunjukkan kebaruan temuan. Dalam konteks CSIRT, peningkatan keamanan siber menjadi perhatian utama karena ancaman siber dapat mengakibatkan kerugian finansial dan non-finansial pada Kementerian Perdagangan. Akuntansi dan big data saling berhubungan dalam penerapan CSIRT. Penggunaan big data dalam CSIRT dapat membantu mengidentifikasi pola dan tren dalam aktivitas siber yang mencurigakan, sehingga tim CSIRT dapat lebih efisien dalam mendeteksi dan mengatasi insiden keamanan siber. Selanjutnya, dengan keamanan siber yang lebih baik, data keuangan organisasi akan lebih terjaga, sehingga memastikan proses akuntansi yang akurat dan transparan. Oleh karena itu CSIRT Kementerian Perdagangan mengemban visi menciptakan keamanan siber yang handal dan terampil di lingkungan Kementerian Perdagangan (Preuveneers, Joosen, Bernal Bernabe, & Skarmeta, 2020). Di samping itu, pembentukan Tim ini juga bertujuan untuk mengkoordinasikan, bekerja sama, dan mengurangi risiko serta memulihkan keamanan siber dengan pihak-pihak publik, privat dan lembaga insiden siber di Indonesia, dan juga bertekad untuk meningkatkan kesadaran dan kualitas layanan TIK di Kementerian Perdagangan atas ancaman siber (Hasumi, Shima, & Takakura, 2019).

Data yang diperoleh pada penelitian yang dilakukan berupa data primer yang diperoleh dengan melakukan wawancara terhadap salah satu anggota CSIRT Kementerian Perdagangan. Pembentukan CSIRT Kementerian Perdagangan diharapkan mampu untuk menjamin penyelenggaraan sistem elektronik terhadap penyediaan pelayanan publik. CSIRT Kementerian Perdagangan memiliki beberapa Layanan, antara lain:

1. Layanan reaktif, yaitu: Pemberian peringatan insider siber (*alerts and warning*), Penyelesaian dan pemulihan jika terjadi insiden siber (*incident handling*) dan penanganan kerawanan siber (*vulnerability handling*), Penanganan artefak (*artifact handling*)
2. Layanan proaktif yaitu audit atau penilaian keamanan siber (*security audit or assessment*)
3. Layanan manajemen kualitas keamanan siber, yaitu: Analisis risiko (*risk analysis*), Edukasi dan pelatihan (*education/training*)

Berdasarkan hasil wawancara, CSIRT Kementerian Perdagangan saat ini dinilai sudah tepat karena dijalankan oleh unit Pusat Data dan Sistem Informasi (PDSI). Hanya saja, CSIRT Kementerian Perdagangan saat ini belum memiliki tim kerja mandiri karena pada pelaksanaannya masih melekat pada tim kerja yang ada pada unit PDSI. Dari sisi pengambil keputusan, sebagai bagian dari unit Eselon II, anggota CSIRT Kementerian Perdagangan bertanggungjawab kepada Kepala PDSI. Kepala PDSI Kementerian Perdagangan dibawahi oleh Sekretaris Jenderal sebagai unit Eselon I di atasnya. Posisi pengambil keputusan unit PDSI dianggap "tidak setingkat" dengan beberapa unit Eselon I lainnya yang dibawahi oleh Direktur Jenderal. Artinya, ketika terjadi masalah siber pada unit eselon I diluar Sekretariat Jenderal, secara birokrasi Kepala PDSI harus melaporkan kepada Eselon I di atasnya yaitu Sekretaris Jenderal agar dapat menyampaikan masalah siber kepada Eselon I lainnya, yang kemudian akan disampaikan kepada unit di bawahnya yang mungkin terdampak serangan siber. Posisi pengambil keputusan merupakan hal yang dapat mempengaruhi pelaksanaan suatu kebijakan, sehingga dari sisi kewenangan, posisi PDSI sebagai unit Eselon II masih dianggap lemah untuk mengatur tingkat Kementerian.

Dalam konteks akuntansi dan big data, hasil penelitian ini menunjukkan bahwa sistem pengelolaan keamanan siber (CSIRT) yang ada di Kementerian Perdagangan saat ini belum optimal. Hal ini disebabkan oleh beberapa faktor, seperti struktur pengambilan keputusan yang birokratis, keterbatasan sumber daya manusia baik dari segi jumlah maupun kompetensi, serta lemahnya kewenangan unit Pusat Data dan Sistem Informasi (PDSI). Dalam era big data, penggunaan dan analisis data yang besar dan kompleks menjadi bagian penting dari berbagai aspek bisnis, termasuk akuntansi (La Fleur, Hoffman, Gibson, & Buchler, 2021). Dalam hal ini, CSIRT memiliki peran penting untuk memastikan keamanan dan integritas data yang digunakan oleh organisasi, termasuk data akuntansi yang menyangkut informasi keuangan dan transaksi bisnis. Ketika terjadi serangan siber, data akuntansi bisa menjadi target dan rentan terhadap manipulasi atau pencurian. Oleh karena itu, dibutuhkan tim CSIRT yang efektif dan efisien dalam mengatasi insiden keamanan siber serta mengambil tindakan penanggulangan dan pemulihan (Ubowska & Królikowski, 2022). Namun, berdasarkan hasil penelitian di atas, terdapat berbagai kendala dalam pelaksanaan CSIRT, seperti lambannya proses pengambilan keputusan dan keterbatasan sumber daya manusia. Sebagai solusi, perlu dilakukan peningkatan pada struktur pengambilan keputusan yang lebih efisien, misalnya dengan memindahkan tim kerja CSIRT di bawah Staf Ahli Menteri Perdagangan yang semula berada di bawah Eselon II untuk mengatur tingkat Kementerian. Selain itu, perlu meningkatkan jumlah dan kompetensi sumber daya manusia yang mengelola CSIRT, agar mampu mengatasi berbagai insiden keamanan siber dengan respons cepat dan efektif. Hal ini penting untuk menjaga keamanan dan integritas data akuntansi, serta memastikan kelancaran bisnis dan kepercayaan stakeholder dalam era big data.

KESIMPULAN

Pembentukan tim CSIRT Kementerian Perdagangan merupakan langkah yang penting dan strategis dalam konteks keamanan siber dan akuntansi di era big data. Namun, berdasarkan hasil penelitian ini, pelaksanaan CSIRT saat ini belum optimal dan tersendat oleh beberapa kendala, seperti struktur pengambilan keputusan yang birokratis, keterbatasan sumber daya manusia, dan lemahnya kewenangan unit PDSI. Untuk mengatasi kendala-kendala tersebut, diperlukan peningkatan struktur pengambilan keputusan, peningkatan jumlah dan kompetensi SDM, serta penerapan teknologi big data yang lebih efektif dan efisien dalam mengelola keamanan siber. Dengan peningkatan ini, diharapkan CSIRT Kementerian Perdagangan dapat menjadi lebih responsif dalam melindungi data akuntansi organisasi serta memastikan kelancaran bisnis dan kepercayaan stakeholder.

Adapun saran dan rekomendasi yang dapat diberikan untuk meningkatkan efektivitas CSIRT di Kementerian Perdagangan antara lain; Mengoptimalkan struktur pengambilan keputusan dengan memindahkan tim kerja CSIRT menjadi di bawah Staf Ahli Menteri Perdagangan untuk mengatur tingkat Kementerian, sehingga proses pengambilan keputusan menjadi lebih efisien dan tidak terhambat oleh birokrasi.

Meningkatkan jumlah dan kompetensi sumber daya manusia yang mengelola CSIRT, agar mampu mengatasi berbagai insiden keamanan siber dengan respons cepat dan efektif. Hal ini dapat dilakukan melalui perekrutan tenaga baru yang ahli di bidang siber, serta penyelenggaraan pelatihan dan pendidikan bagi tenaga yang ada untuk meningkatkan pengetahuan dan keterampilan mereka dalam menghadapi ancaman siber. Mengembangkan kapasitas dan kewenangan unit PDSI dalam mengelola CSIRT, sehingga dapat lebih efektif dalam mengatasi insiden siber dan mengambil tindakan preventif untuk melindungi data akuntansi dan big data.

Meningkatkan kerjasama antar instansi dan sektor swasta dalam konteks keamanan siber, baik di tingkat nasional maupun internasional, sehingga dapat saling bertukar informasi dan *best practice* dalam menghadapi ancaman siber yang semakin kompleks. Kemudian melakukan penilaian dan evaluasi secara berkala terhadap pelaksanaan CSIRT, guna mengidentifikasi kelemahan dan peluang perbaikan, serta memastikan keberlanjutan dan peningkatan kinerja CSIRT dalam menghadapi tantangan keamanan siber yang terus berkembang. Dengan menerapkan saran dan rekomendasi tersebut di atas, diharapkan CSIRT Kementerian Perdagangan dapat menjadi lebih efektif dan efisien dalam menghadapi ancaman siber, sehingga mampu melindungi keamanan dan integritas data akuntansi serta memastikan kelancaran bisnis dan kepercayaan stakeholder dalam era big data.

DAFTAR PUSTAKA

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 13(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Alzubaidi, L., Bai, J., Al-Sabaawi, A., Santamaría, J., Albahri, A. S., Al-dabbagh, B. S. N., … Gu, Y. (2023). A survey on deep learning tools dealing with data scarcity: definitions, challenges, solutions, tips, and applications. Journal of Big Data, 10(1), 1–82. https://doi.org/10.1186/s40537-023-00727-2

Amanowicz, M. (2021). A shared cybersecurity awareness platform. Journal of Telecommunications and Information Technology, 2021(3), 32–41. https://doi.org/10.26636/JTIT.2021.154421

Annef, A. B. (2021). Ancaman Siber Di Tengah Pandemi Covid-19 : Tinjauan Terhadap Keamanan Non-Tradisional Dan Keamanan Siber Di Indonesia. Sriwijaya Journal of International Relations, 1(1), 34–49.

Babys, S. A. M. (2021). Ancaman Perang Siber di Era Digital dan Solusi Keamanan Indonesia. Jurnal Oratio Directa, 3(1), 425–442. Retrieved from https://ejurnal.ubk.ac.id/index.php/oratio/article/view/163

Badan Siber dan Sandi Negara. (2020). Patent No. 10. Indonesia.

Badan Siber dan Sandi Negara. (2021). Patent No. 6. Indonesia.

Berardi, D., Tippenhauer, N. O., Melis, A., Prandini, M., & Callegati, F. (2023). Time sensitive networking security: issues of precision time protocol and its implementation. Cybersecurity, 6(1). https://doi.org/10.1186/s42400-023-00140-5

Bhardwaj, A., & Sapra, V. (2021). Authentication Attacks. In EAI/Springer Innovations in Communication and Computing. https://doi.org/10.1007/978-3-030-69174-5_11

Chałubińska-Jentkiewicz, K., Radoniewicz, F., & Zieliński, T. (2022). Cybersecurity in Poland: Legal Aspects. In Springer. Poland: Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-030-78551-2_5

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 10(2), 113–128. https://doi.org/10.22212/jp.v10i2.1447

Hasumi, D., Shima, S., & Takakura, H. (2019). SPINZ: A speculating incident zone system for incident handling. Journal of Cyber Security and Mobility, 8(3), 341–364. https://doi.org/10.13052/jcsm2245-1439.833

Indramawan, D., Handayanto, A. B., & Djajanti, A. (2021). Pentingnya Opini Audit sebagai Pemediasi Peningkatan Indeks Pembangunan Manusia. Jurnal Riset Dan Aplikasi: Akuntansi Dan Manajemen, 5(2), 209–218. https://doi.org/10.33795/jraam.v5i2.007

Kementerian Perdagangan Republik Indonesia. (2021). Profil CSIRT (Computer Security Incident Responsive Team). Retrieved June 11, 2023, from csirt.kemendag.go.id website: https://csirt.kemendag.go.id/portal/profil

La Fleur, C., Hoffman, B., Gibson, C. B., & Buchler, N. (2021). Team performance in a series of regional and national US cybersecurity defense competitions: Generalizable effects of training and functional role specialization. Computers and Security, 104(1), 1–18. https://doi.org/10.1016/j.cose.2021.102229

Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (2021). Ancaman dan Solusi Serangan Siber di Indonesia. Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT), 1(2), 85–92. Retrieved from http://ejournal.upi.edu/index.php/TELNECT/

Pemerintah Pusat. (2018). Peraturan Presiden (PERPRES) Nomor 95 Tahun 2018: Sistem Pemerintahan Berbasis Elektronik. Indonesia: 95.

Prabaswari, P., Alfikri, M., & Ahmad, I. (2022). Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. Matra Pembaruan, 6(1), 1–14. https://doi.org/10.21787/mp.6.1.2022.1-14

Preuveneers, D., Joosen, W., Bernal Bernabe, J., & Skarmeta, A. (2020). Distributed Security Framework for Reliable Threat Intelligence Sharing. Security and Communication Networks, 1(1), 1–15. https://doi.org/10.1155/2020/8833765

Rai, I. N. A. S., Heryadi, D., & Kamaluddin N., A. (2022). The Role of Indonesia to Create Security and Resilience in Cyber Spaces [Peran Indonesia dalam Membentuk Keamanan dan Ketahanan di Ruang Siber]. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 13(1), 43–66. https://doi.org/10.22212/jp.v13i1.2641

Ubowska, A., & Królikowski, T. (2022). Building a cybersecurity culture of public administration system in Poland. Procedia Computer Science, 207(1), 1242–1250. https://doi.org/10.1016/j.procs.2022.09.180

Wulandari, S. S. (2023). Big Data Concepts , Opportunities, Challenges, and Paradoxes. BULLET : Jurnal Multidisiplin Ilmu, 2(01), 1–5.

Zhang, Y., & Dong, H. (2023). Criminal law regulation of cyber fraud crimes—from the perspective of citizens' personal information protection in the era of edge computing. Journal of Cloud Computing, 12(1), 1–17. https://doi.org/10.1186/s13677-023-00437-3.