Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id

E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari

OPEN ACCESS

https://doi.org/10.35870/jimik.v6i1.1210

Kajian Strategik Manajemen Keamanan Siber terhadap Proyek Telematika di Indonesia: Studi Kasus Kebocoran Pusat Data Nasional

Eka Hero Ramadhani [1*], I Ketut Agung Enriko [2], Erika Lety Istikhomah Puspita Sari [3]

[1*] Program Studi Magister Terapan Teknik Elektro, Politeknik Negeri Jakarta, Kota Depok, Provinsi Jawa Barat, Indonesia.
[2] Fakultas Teknik Elektro, Telkom University, Kota Bandung, Provinsi Jawa Barat, Indonesia.
[3] Research and Innovation Management, Telkom Corporate University, Kota Bandung, Provinsi Jawa Barat, Indonesia.

Email: eka.hero.ramadhani.te23@stu.pnj.ac.id [1*], iketutagungenriko@telkomuniversity.ac.id [2], erika.lety@itdri.id [3]

Histori Artikel:
Dikirim 16 Desember 2024; *Diterima dalam bentuk revisi* 23 Desember 2024; *Diterima* 1 Januari 2025; *Diterbitkan* 10 Januari 2025.

Abstrak

Pada tanggal 20 Juni 2024 terjadi serangan siber pada Pusat Data Nasional (PDN) yang menyebabkan beberapa layanan publik pemerintah berupa Sistem Pemerintahan Berbasis Elektronik (SPBE) tidak berjalan dengan baik. Insiden tersebut berpotensi menyebabkan kebocoran dan penyalahgunaan data pemerintah maupun masyarakat Indonesia oleh peretas. Kasus insiden siber pada PDN perlu dikaji guna mendapatkan pengetahuan yang bermanfaat untuk penyelenggaraan keamanan siber pada proyek telematika di Indonesia, khususnya SPBE. Dalam makalah ilmiah ini dilakukan kajian stratejik manajemen keamanan siber terhadap proyek telematika di Indonesia dengan studi kasus kebocoran PDN. Metode studi eksplorasi digunakan untuk identifikasi penyebab insiden siber pada PDN. Faktor-faktor penyebab insiden siber PDN selanjutnya dipetakan ke dalam kerangka kerja People, Process, and Technology (PPT) untuk ditentukan solusi penanganannya. Hasil identifikasi dan pemetaan menunjukkan bahwa terdapat sebanyak 3 faktor manusia, 4 faktor proses, dan 7 faktor teknologi. Strategi manajemen keamanan siber untuk proyek telematika di Indonesia yang diusulkan dalam kajian ini berupa solusi-solusi penanganan, mitigasi, dan antisipasi insiden siber sesuai studi kasus yang dikaji. Hasil kajian ini dapat menjadi rujukan bagi penyelenggara proyek telematika layanan publik selanjutnya supaya tidak terjadi insiden siber serupa di kemudian hari.

Kata Kunci: Keamanan Siber; Manajemen; PDN; Proyek Telematika; Serangan Siber.

Abstract

On June 20, 2024, a cyber attack occurred on PDN, which caused several government public services in the form of SPBE to not run properly. The incident has the potential to cause data leakage and disclosure of the government and the Indonesian public by hackers. Cyber incident cases on PDN need to be studied in order to gain useful knowledge for implementing cybersecurity in telematics projects in Indonesia, especially SPBE. In this scientific paper, a study of cybersecurity management strategies is conducted on telematics projects in Indonesia with a case study of PDN leaks. The exploratory study method is used to identify the causes of cyber incidents on PDN. The factors causing PDN cyber incidents are then entered into the PPT framework to determine the handling solutions. The results of the identification and mapping show that there are 3 human factors, 4 factors, and 7 technological factors. The cybersecurity management strategy for telematics projects in Indonesia proposed in this study is in the form of solutions for handling, mitigating, and anticipating cyber incidents according to the case study studied. The results of this study can be a reference for organizers of public service telematics projects so that similar incidents do not occur in the future.

Keyword: Cyber Attack; Cyber Security; Management; PDN; Telematics Project.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1210

1. Pendahuluan

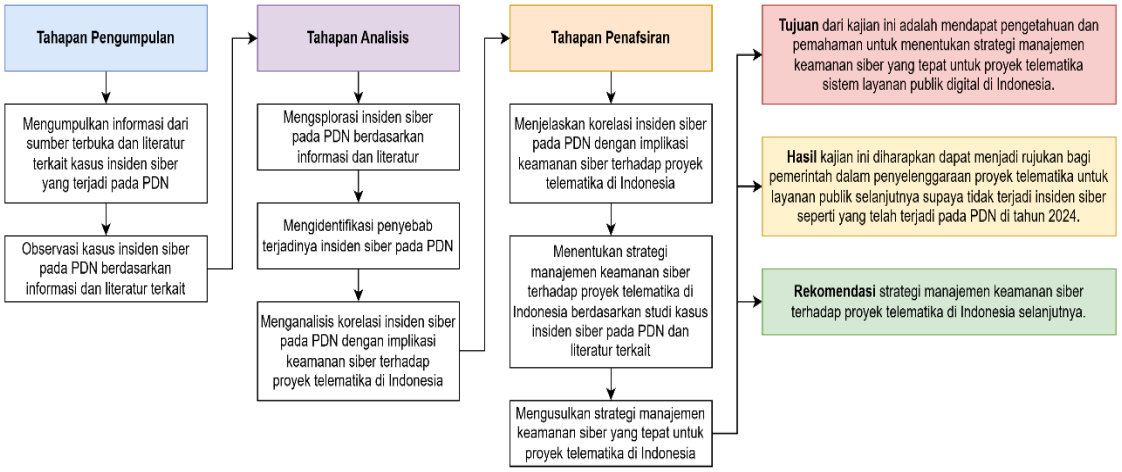
Perkembangan infrastruktur Teknologi Informasi dan Komunikasi (TIK) di era modern mendorong pemerintah untuk melakukan digitalisasi proses administrasi (Jou *dkk*., 2024). Administrasi pemerintahan memanfaatkan TIK terkini untuk meningkatkan efisiensi pelayanan publik, memperluas jangkauan layanan, menyediakan layanan secara daring, dan meningkatkan partisipasi warga negara serta pemangku kepentingan dalam penyelenggaraan layanan publik (Xue *dkk*., 2024; Güler & Büyüközkan, 2023; Medaglia *dkk*., 2021; Scholl, 2020). Sistem pengelolaan layanan publik berbasis TIK bertujuan meningkatkan kualitas, manajemen, transparansi, dan mutu layanan bagi pemangku kepentingan, termasuk kementerian/lembaga, badan pemerintahan, perusahaan, dan masyarakat (Sapraz & Han, 2024; Ashaye & Irani, 2019). Penyelenggaraan sistem ini di Indonesia diatur dalam Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) (Presiden Republik Indonesia, 2018). SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan TIK untuk menyediakan layanan kepada penggunanya. Tujuan SPBE meliputi tata kelola pemerintahan yang bersih, efektif, efisien, transparan, dan akuntabel; layanan publik yang berkualitas dan terpercaya; serta sistem pemerintahan berbasis elektronik yang terintegrasi. Pemerintah memerlukan infrastruktur yang mencakup perangkat keras, perangkat lunak, dan fasilitas pendukung seperti sistem aplikasi, pengolahan dan penyimpanan data, komunikasi data, penghubung, serta perangkat elektronik lainnya (Presiden Republik Indonesia, 2018). Infrastruktur utama SPBE meliputi Pusat Data Nasional (National Data Center atau PDN), jaringan intra-pemerintah, dan sistem penghubung layanan pemerintah. Dalam arsitektur ini, PDN berfungsi sebagai pengelola, penyimpan, dan pemulih data SPBE (Presiden Republik Indonesia, 2022). Data yang dikelola mencakup informasi masyarakat, pelaku usaha, atau pemangku kepentingan lainnya, yang menjadi aset penting dalam SPBE. Oleh karena itu, keamanan dan perlindungan data adalah aspek fundamental dalam penyelenggaraan SPBE (Rahman, 2021). Desain dan implementasi sistem ini harus mempertimbangkan keamanan data, mengingat sifat sensitifnya (Ibrahim *dkk*., 2020). Pemerintah sebagai penyelenggara SPBE wajib menerapkan sistem keamanan siber untuk mencegah kebocoran data akibat peretasan. Data pribadi masyarakat dapat disalahgunakan untuk kejahatan seperti penipuan, pemerasan, dan pencurian, yang berpotensi menimbulkan kerugian finansial maupun reputasi.

Pada 20 Juni 2024, terjadi serangan siber terhadap PDN yang menyebabkan beberapa layanan SPBE tidak berfungsi dengan baik, sekaligus meningkatkan risiko kebocoran data masyarakat akibat peretasan (Ramdhan *dkk*., 2024; Khoerunisa, 2024; Ardipandanto, 2024). Insiden ini menjadi ancaman serius bagi keamanan data pemerintah dan masyarakat (Mayda & Elvaretta, 2024). Peretas berhasil mengakses sistem PDN, mengunci data menggunakan *ransomware*, sehingga data tidak dapat diproses oleh aplikasi SPBE dan menyebabkan terganggunya beberapa layanan publik (CNN Indonesia, 2024; Rahayu, 2024; SAFEnet, 2024). Permasalahan diperparah oleh ketiadaan sistem *backup* data yang diterapkan dalam pengelolaan teknis PDN (Emedia DPR RI, 2024a; Yesidora, 2024). Pemerintah harus segera menerapkan strategi manajemen risiko dan krisis untuk menghadapi ancaman serangan siber yang semakin kompleks (Skierka, 2023). Komisi I DPR RI bahkan mendesak pembentukan pusat krisis dan satuan tugas (*task force*) khusus untuk menangani kasus serupa di masa mendatang (Emedia DPR RI, 2024b). Penelitian terhadap insiden siber pada PDN menjadi relevan untuk memahami langkah-langkah yang dapat meningkatkan keamanan dalam penyelenggaraan layanan berbasis TIK di Indonesia, khususnya proyek telematika. Penelitian ini menganalisis strategi manajemen keamanan siber dalam proyek telematika dengan studi kasus kebocoran PDN. Analisis dilakukan untuk mengidentifikasi penyebab insiden siber, menyusun strategi keamanan yang tepat, dan merekomendasikan langkah manajemen proyek telematika agar insiden serupa tidak terulang. Pendekatan eksplorasi digunakan dalam penelitian ini dengan memanfaatkan literatur yang relevan. Hasil kajian diharapkan menjadi rujukan bagi pemerintah dalam penyelenggaraan proyek telematika untuk mendukung keamanan layanan publik secara berkelanjutan.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1210

2. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah eksplorasi. Pendekatan ini dirancang untuk memahami suatu sistem secara menyeluruh (Ramadhani *dkk*., 2024). Fokus utama metode eksplorasi adalah pada evaluasi dan analisis data, bukan pada pembuatan desain atau model baru (Ramadhani & Wulandari, 2024). Metode ini diterapkan untuk mengamati, mempelajari, dan memahami fenomena atau sistem guna memperoleh pemahaman yang lebih baik mengenai subjek penelitian (Edgar & Manz, 2017). Dalam ilmu sosial, metode eksplorasi sering dianggap sebagai pendekatan kualitatif. Hasil eksplorasi biasanya berupa analisis data yang tidak berada di bawah kendali langsung peneliti, sering kali disebut sebagai data sekunder yang dikumpulkan setelah kejadian. Metode ini sangat berguna untuk menemukan informasi terkait sistem atau fenomena yang variabelnya tidak dapat dikendalikan, seperti insiden keamanan siber. Contohnya adalah ancaman atau serangan siber yang terjadi secara acak dan sulit diprediksi. Pendekatan eksplorasi meliputi kegiatan pengumpulan, analisis, dan interpretasi data terkait desain, sistem, model, teori, atau subjek tertentu untuk memperluas pemahaman. Tahapan penelitian ini mengacu pada metode eksplorasi yang melibatkan tiga langkah utama: pengumpulan data, analisis, dan interpretasi kasus kebocoran *Pusat Data Nasional* (PDN) serta implikasinya terhadap keamanan siber dalam proyek telematika layanan publik di Indonesia. Tujuan utama penelitian ini adalah untuk memperoleh pemahaman yang jelas guna menyusun strategi manajemen keamanan siber yang efektif pada proyek telematika layanan publik digital di Indonesia. Diagram tahapan penelitian ini disajikan pada gambar 1.



Gambar 1. Diagram Tahapan Kajian Stratejik Manajemen Keamanan Siber terhadap Proyek Telematika di Indonesia

3. Hasil dan Pembahasan

3.1 Hasil

3.1.1 Identifikasi Penyebab Insiden Siber pada PDN Indonesia

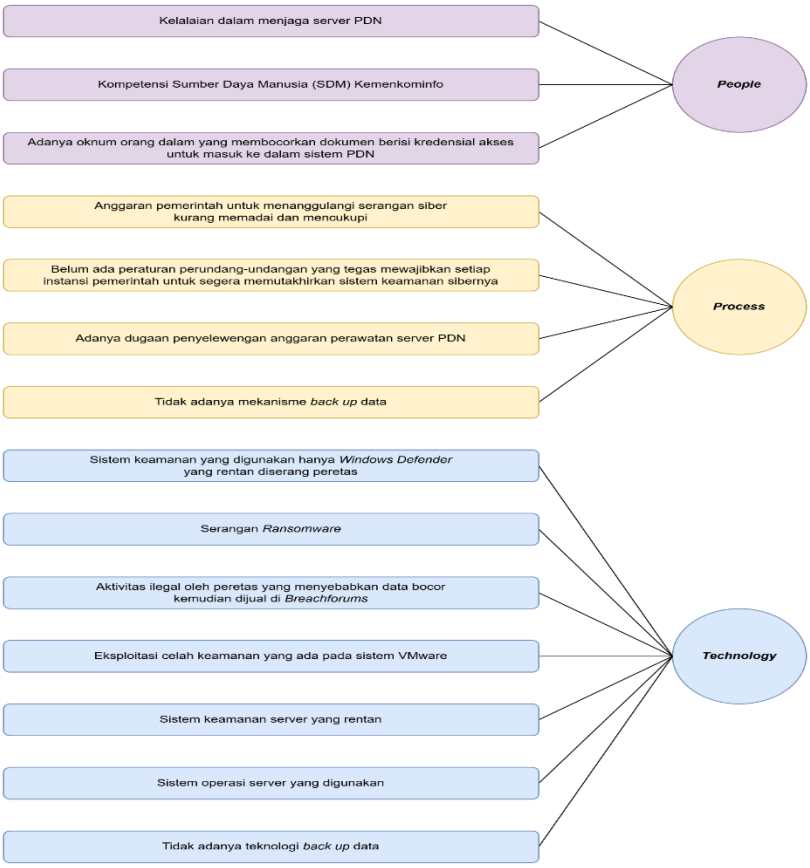
Insiden serangan siber yang menimpa Pusat Data Nasional (PDN) di Indonesia menjadi salah satu contoh nyata lemahnya kesiapan infrastruktur keamanan siber pemerintah dalam menghadapi ancaman yang semakin kompleks. Berdasarkan laporan dari Pusat Analisis Keparlemenan Badan Keahlian DPR RI, terdapat tiga faktor utama yang menyebabkan lemahnya sistem keamanan PDN terhadap serangan siber (Ardipandanto, 2024). Pertama, sistem keamanan yang digunakan hanya bergantung pada *Windows Defender*, yang dikenal memiliki kelemahan dan rentan terhadap serangan.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1210

Kedua, anggaran yang dialokasikan oleh pemerintah untuk mengelola dan meningkatkan keamanan siber dinilai tidak mencukupi. Ketiga, belum adanya regulasi yang mengharuskan setiap instansi pemerintah untuk secara rutin memperbarui sistem keamanan mereka sesuai dengan perkembangan teknologi. Sumber lain mengungkapkan bahwa kelemahan dalam pengelolaan server juga turut berkontribusi terhadap terjadinya insiden ini. Ramadhan *dkk*. menyebutkan bahwa kelalaian dalam pengelolaan server PDN, termasuk adanya indikasi penyelewengan anggaran untuk perawatan server, menjadi salah satu pemicu utama kebocoran data tersebut (Ramdhan *dkk*., 2024). Informasi lebih lanjut dari Khoerunisa menyoroti serangan *ransomware* sebagai metode utama yang digunakan peretas, yang tidak hanya mengakibatkan kebocoran data, tetapi juga menyebabkan data tersebut dijual di platform gelap seperti *Breachforums*. Selain itu, sistem *VMware* yang digunakan oleh PDN juga memiliki celah keamanan yang dieksploitasi oleh pelaku serangan (Khoerunisa, 2024). Pakar keamanan siber dari Lembaga Riset Keamanan Siber CISSReC menjelaskan bahwa serangan yang terjadi pada PDN memiliki karakteristik serangan *ransomware*. Pola serangan ini terlihat dari lamanya waktu pemulihan sistem setelah gangguan terjadi (Muslim, 2024). Analisis lebih lanjut oleh Lukman Hakim, pakar IT dari Universitas Muhammadiyah Surabaya, mengidentifikasi empat faktor tambahan yang berkontribusi terhadap insiden ini, yaitu rendahnya kompetensi sumber daya manusia (SDM), kerentanan sistem keamanan server, penggunaan sistem operasi yang kurang aman, dan ketiadaan mekanisme *backup* data (Savitri, 2024). Hidayat dan Allan juga menegaskan bahwa serangan *ransomware* adalah salah satu ancaman terbesar yang dihadapi oleh PDN (Hidayat & Allan, 2024).

Dalam konferensi pers, Kepala Badan Siber dan Sandi Negara (BSSN) mengungkapkan bahwa serangan *ransomware* yang menyerang PDN diidentifikasi sebagai *Brain Cipher Ransomware* (BCR) (Puspapertiwi & Dzulfaroh, 2024). Pakar Teknik Informatika dari Institut Teknologi Bandung, Yudistira Dwi Wardhana Asnar, menjelaskan bahwa serangan ini memanfaatkan celah keamanan tertentu dalam sistem untuk mengenkripsi data, sehingga tidak dapat diakses oleh pemilik sahnya. Di sisi lain, laporan dari berbagai media massa seperti Liputan6, Kompas, dan IDN Times menyoroti peran oknum orang dalam yang diduga membocorkan dokumen berisi kredensial akses ke sistem PDN, yang semakin memperparah situasi (Yuslianson, 2024; Clinten & Pertiwi, 2024; Lidyana, 2024). Untuk memahami akar penyebab insiden ini secara terstruktur, penelitian ini memanfaatkan kerangka kerja PPT (*People, Process, Technology*). Kerangka kerja ini berfokus pada keseimbangan antara keterampilan dan keahlian manusia, prosedur dan kebijakan operasional, serta teknologi pendukung sistem untuk memastikan efektivitas strategi dan keberlanjutan pengelolaan aset Teknologi Informasi (TI) (Ferdynandus *dkk*., 2024). Ketiga aspek ini saling berkaitan dan memiliki peran penting dalam melindungi sistem dan infrastruktur SPBE (*Sistem Pemerintahan Berbasis Elektronik*) dari ancaman siber secara efektif (Handri *dkk*., 2023). Meskipun teknologi sering dianggap sebagai solusi utama untuk memitigasi ancaman siber, penelitian menunjukkan bahwa manusia menjadi penyebab utama dalam 85% pelanggaran data. Faktor manusia mencakup pencurian kredensial, phishing, penyalahgunaan, atau kesalahan yang tidak disengaja. Selain itu, aspek proses juga memegang peranan penting dalam menjamin keamanan sistem melalui prosedur operasional yang baik, kebijakan yang memadai, dan tata kelola yang konsisten. Oleh karena itu, analisis berbasis PPT dapat membantu mengidentifikasi dan mengklasifikasikan jenis ancaman, serta merancang solusi dan langkah mitigasi yang relevan (Ghaffari *dkk*., 2019). Dalam penelitian ini, data yang telah dikumpulkan dari sumber terbuka dan literatur terkait dipetakan ke dalam kerangka kerja PPT untuk memudahkan identifikasi penyebab insiden serta klasifikasinya. Misalnya, penggunaan *Windows Defender* sebagai satu-satunya sistem keamanan PDN masuk dalam kategori kelemahan teknologi. Diagram pemetaan penyebab insiden siber pada PDN ke dalam kerangka kerja PPT disajikan pada gambar 2. Pendekatan ini diharapkan mampu memberikan panduan yang jelas bagi pemerintah dan pemangku kepentingan dalam merancang strategi mitigasi dan antisipasi serangan siber. Dengan memahami faktor manusia, proses, dan teknologi secara komprehensif, upaya peningkatan keamanan PDN dapat dilakukan secara lebih efektif dan berkelanjutan.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1210



Gambar 2. Diagram Pemetaan Penyebab Insiden Siber pada PDN ke dalam Kerangka Kerja PPT

Hasil pemetaan penyebab insiden siber pada PDN ke dalam kerangka kerja PPT yang telah disajikan dalam bentuk diagram menunjukkan bahwa terdapat sebanyak 3 faktor manusia, 4 faktor proses, dan 7 faktor teknologi. Pemetaan faktor penyebab insiden siber pada PDN ke dalam kerangka kerja PPT yang dilakukan dalam kajian ini memudahkan untuk klasifikasi faktor-faktor penyebab terjadinya insiden siber pada PDN berdasarkan kerangka kerja PPT sehingga memudahkan untuk analis dan menentukan solusi penanganan dan mitigasinya. Selain itu, hasil identifikasi penyebab terjadinya insiden siber pada PDN juga akan memudahkan dalam analisis korelasi implikasi keamanan siber terhadap proyek telematika di Indonesia, khususnya proyek penyelenggaraan SPBE.

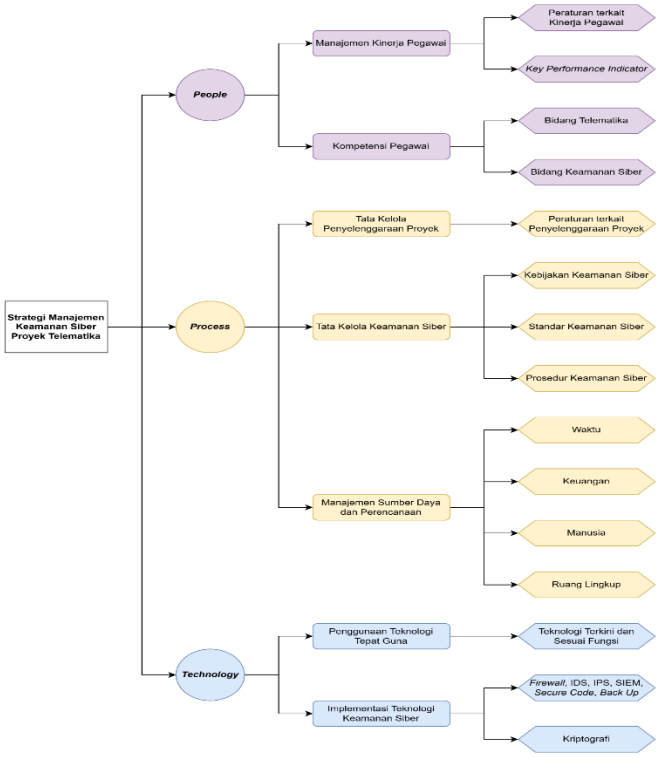
3.1.2 Implikasi Keamanan Siber terhadap Proyek Telematika di Indonesia

Penetapan prioritas penerapan keamanan siber seperti kerangka kerja PPT dalam SPBE memiliki implikasi yang cukup besar terhadap keberhasilan perlindungan data dan informasi (Handri *dkk*., 2023). Kegagalan dalam penerapan keamanan siber pada proyek telematika di Indonesia dapat menyebabkan berbagai macam dampak buruk. Misalnya, turunnya tingkat kepercayaan masyarakat kepada Pemerintah Indonesia karena tidak mampu menjaga keamanan siber SPBE yang diselenggarakannya sehingga data masyarakat bocor dan disalahgunakan oleh peretas. Selain itu, Negara Indonesia dapat dianggap tidak mampu melindungi data nasionalnya. Reputasi buruk tersebut dapat menghambat kerja sama internasional dan investasi dari negara lain sehingga berpotensi mempengaruhi pertumbuhan ekonomi Negara Indonesia (Ihsan & Sekti, 2024). Dampak lain dari insiden siber pada PDN adalah terganggunya beberapa layanan SPBE yang menggunakan infrastruktur PDN (Adristi & Ramadhani, 2024). Terganggunya layanan SPBE dapat menyebabkan lambatnya proses bisnis pelayanan publik. Hal itu akan berdampak pada turunnya kualitas layanan publik yang diselenggarakan oleh pemerintah yang mungkin juga akan berdampak pada kerugian

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1210

finansial atau ekonomi masyarakat. Oleh sebab itu, keamanan siber penting untuk diterapkan pada penyelenggaraan proyek telematika di Indonesia seperti penyelenggaraan SPBE untuk layanan publik. Penyelenggaraan proyek telematika di Indonesia harus menerapkan manajemen yang tepat dan strategis, khususnya dalam hal manajemen penerapan keamanan siber pada proyek telematika untuk menghadapi tantangan serangan siber yang semakin hari semakin masif dan maju. Apabila vendor penyelenggara proyek telematika tidak menerapkan manajemen yang baik dan keamanan siber pada proyeknya, maka proyek yang dikembangkan akan rentan terhadap serangan siber.

Dampak buruk dari manajemen proyek telematika yang tidak baik adalah hasil proyek yang dibangun atau dikembangkan tidak memenuhi standar kualitas layanan dan keamanan dari proyek itu sendiri, akibatnya dapat menurunkan kepuasan dan kepercayaan pengguna layanan (masyarakat) terhadap penyelenggara proyek telematika (pemerintah atau vendor). Reputasi penyelenggara proyek telematika bergantung pada hasil dan kualitas proyek yang dikerjakannya. Penyelenggara proyek telematika harus baik dan tepat dalam memanajemen proyeknya. Tujuan penerapan keamanan siber untuk mencapai 3 aspek utama yaitu *Confidentiality*, *Integrity*, *and Availability* (CIA) (Taherdoost, 2022). Aspek *Confidentiality* berkaitan dengan kerahasiaan data yang ditransmisikan, diproses, dikelola, dan disimpan dalam suatu sistem siber dengan tujuan data tidak dapat dibaca oleh pihak yang tidak berwenang dalam suatu sistem sehingga tidak dapat disalahgunakan. Aspek *Integrity* berkaitan dengan keaslian dan keutuhan data yang berarti data tidak dimodifikasi oleh pihak tidak berwenang dalam suatu sistem siber. Aspek *Availability* berkaitan dengan jaminan keteraksesan dan ketersediaan data untuk diproses dan diakses oleh sistem dan pengguna. Sistem siber merupakan luaran dari proyek telematika. Untuk menghasilkan sistem siber yang baik dan aman, maka penyelenggaraan dan manajemen proyek telematika harus menerapkan keamanan siber. Manajer proyek telematika dapat menggunakan kerangka kerja PPT sebagai strategi manajemen keamanan siber proyek telematika. Diagram penerapan kerangka kerja PPT untuk strategi manajemen keamanan siber proyek telematika disajikan pada gambar 3.



Gambar 3. Diagram Penerapan Kerangka Kerja PPT untuk Strategi Manajemen Keamanan Siber Proyek Telematika

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1210

Menghadapi tantangan keamanan siber yang meliputi ancaman dan serangannya memerlukan pengetahuan yang tepat tentang berbagai persoalan keamanan siber dan ruang lingkup solusinya. Keamanan siber dalam proyek telematika merupakan produk jangka panjang dari kolaborasi antara manusia, proses, dan teknologi dalam suatu sistem. Identifikasi dan kategorisasi berdasarkan kerangka kerja PPT memungkinkan dan memudahkan untuk menentukan solusi dari masalah keamanan siber. Dengan identifikasi dan klasifikasi ancaman serangan siber dalam ketiga area PPT dapat membantu para manajer proyek telematika dalam menyelesaikan masalah keamanan siber. Dalam penelitian ini membahas implikasi keamanan siber dengan menggunakan pendekatan kerangka kerja PPT pada proyek telematika di Indonesia dengan studi kasus insiden kebocoran data PDN Indonesia. Pembahasan komprehensif dalam kajian ini diharapkan dapat digunakan untuk menemukan solusi yang tepat dan efisien.

3.1.3 Strategi Manajemen Keamanan Siber untuk Proyek Telematika di Indonesia

Kegagalan proyek pemerintahan digital sering kali disebabkan oleh faktor nonteknis seperti keterbatasan pada aspek manusia, manajemen, jaringan organisasi, dan dinamika politik (Luna-Reyes *dkk*., 2021). Faktor manusia mencakup individu-individu yang terlibat dalam pengelolaan proyek telematika dan keamanan siber. Pengelolaan Sistem Pemerintahan Berbasis Elektronik (SPBE) tidak hanya menjadi tanggung jawab operator atau divisi Teknologi Informasi (TI), tetapi juga melibatkan seluruh pegawai dan manajer dalam organisasi (Handri *dkk*., 2023). Oleh karena itu, pengelolaan sumber daya manusia menjadi salah satu prioritas penting dalam strategi manajemen keamanan siber. Hal ini menjadi lebih krusial mengingat individu memiliki peran sentral dalam penyelenggaraan dan pengelolaan proyek telematika, baik sebagai penyelenggara, pengelola, maupun pengguna layanan. Berdasarkan analisis penyebab insiden siber di PDN, ditemukan bahwa terdapat tiga faktor utama pada aspek manusia yang perlu ditangani, yaitu kelalaian dalam menjaga server, rendahnya kompetensi SDM, dan keterlibatan oknum yang membocorkan kredensial akses ke sistem PDN. Ketiga masalah ini perlu segera diatasi agar tidak menimbulkan insiden serupa di masa mendatang. Beberapa langkah yang dapat diambil meliputi penyuluhan kesadaran keamanan siber, pelatihan tata kelola dan teknis keamanan, peningkatan kesejahteraan pegawai, pembatasan hak akses berdasarkan kewenangan, dan penerapan evaluasi kinerja secara berkala.

Selain faktor manusia, aspek proses juga memegang peran penting dalam keberhasilan manajemen keamanan siber pada proyek telematika. Identifikasi penyebab insiden di PDN menunjukkan bahwa terdapat empat kelemahan utama pada aspek ini, yaitu minimnya alokasi anggaran untuk keamanan siber, ketiadaan regulasi wajib untuk pemutakhiran sistem keamanan, dugaan penyelewengan anggaran perawatan server, dan tidak adanya mekanisme *backup* data. Untuk mengatasi hal ini, langkah strategis yang dapat dilakukan mencakup penerapan regulasi yang telah ditetapkan, seperti Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE, penyusunan anggaran yang memadai untuk kebutuhan keamanan, audit keuangan yang objektif dan berintegritas, serta penerapan mekanisme *backup* data dan kontrol akses yang sesuai standar. Selain itu, kebijakan untuk pembaruan sistem secara berkala dan rekrutmen SDM yang berintegritas perlu menjadi prioritas, diiringi dengan audit dan evaluasi keamanan secara rutin guna memastikan sistem tetap dalam kondisi optimal. Aspek teknologi juga menjadi salah satu pilar penting dalam kerangka kerja PPT (*People, Process, Technology*). Berdasarkan analisis, terdapat tujuh faktor yang berkontribusi terhadap kelemahan sistem PDN, yaitu ketergantungan pada Windows Defender yang rentan, serangan *ransomware*, aktivitas ilegal peretas yang menyebabkan kebocoran data, eksploitasi celah keamanan pada sistem VMware, sistem operasi server yang tidak aman, kerentanan server, dan tidak adanya teknologi *backup* data. Strategi yang diusulkan untuk menangani kelemahan ini mencakup penggunaan perangkat keamanan siber seperti *firewall*, IDS, IPS, dan SIEM untuk memonitor dan menangkal serangan yang masuk ke sistem. Selain itu, penerapan *secure coding* pada aplikasi, konfigurasi file yang aman, pembaruan sistem operasi secara rutin dengan rekomendasi penggunaan Linux, dan patching aplikasi adalah langkah penting lainnya. Sistem akses kontrol yang ketat untuk pengguna, penyediaan teknologi *backup* data, serta enkripsi menggunakan sistem kriptografi juga diperlukan untuk menjamin

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1210

kerahasiaan data. Lebih jauh lagi, integrasi teknologi keamanan dengan *Machine Learning* (ML) dan *Artificial Intelligence* (AI) dapat membantu memprediksi dan mengatasi ancaman siber yang semakin kompleks di masa depan. Penerapan strategi manajemen keamanan siber yang holistik berdasarkan kerangka kerja PPT ini dapat menjadi landasan yang kuat bagi pemerintah dan penyelenggara proyek telematika di Indonesia. Dengan mengatasi kelemahan pada aspek manusia, proses, dan teknologi, sistem keamanan yang lebih tangguh dapat diwujudkan, sehingga melindungi data sensitif masyarakat dan infrastruktur digital nasional dari ancaman yang terus berkembang.

3.2 Pembahasan

Serangan siber pada Pusat Data Nasional (PDN) menyoroti kelemahan fundamental dalam tata kelola keamanan siber pemerintah, baik dari segi teknis maupun nonteknis. Penelitian Adristi dan Ramadhani (2024) menunjukkan bahwa insiden ini mencerminkan kurangnya penguatan budaya keamanan siber dalam organisasi, khususnya di sektor pemerintahan. Melalui pendekatan dimensi budaya Hofstede, mereka menekankan bahwa organisasi di Indonesia sering mengabaikan aspek proaktif dalam pengelolaan keamanan siber, yang berlawanan dengan pendekatan berbasis teknologi canggih di negara maju. Penelitian ini memperkuat temuan sebelumnya oleh Edgar dan Manz (2017), yang menyatakan bahwa keamanan siber memerlukan kombinasi faktor teknis dan manusia. Namun, dibandingkan dengan penelitian Edgar dan Manz yang lebih berfokus pada pendekatan teknologi seperti integrasi *firewall*, enkripsi, dan sistem deteksi dini, penelitian ini menambahkan elemen budaya dan regulasi sebagai aspek yang lebih dominan dalam kelembagaan di Indonesia. Hal ini relevan dengan kritik dari BSSN (Badan Siber dan Sandi Negara), yang menyebutkan bahwa ketiadaan sistem *backup* data dan lemahnya regulasi pengelolaan sistem menjadi penyebab utama kerentanan PDN (Yesidora, 2024). Dibandingkan dengan penelitian Ghaffari *dkk*. (2019), yang berfokus pada kerangka kerja *People, Process, Technology* (PPT) dalam keamanan cloud, penelitian ini memberikan perspektif yang lebih terperinci terkait implementasi PPT pada proyek telematika pemerintahan. Penelitian Ghaffari menyoroti pentingnya integrasi teknologi mutakhir, seperti *Machine Learning* (ML) dan *Artificial Intelligence* (AI), untuk mendeteksi dan mengatasi ancaman siber secara proaktif. Sementara itu, penelitian ini menekankan bahwa meskipun teknologi menjadi pilar penting, kelemahan pada aspek manusia dan proses, seperti rendahnya literasi digital dan ketidakkonsistenan regulasi, tetap menjadi penyebab dominan terjadinya insiden.

Perbandingan juga dapat dilakukan dengan penelitian Ashaye dan Irani (2019), yang menyoroti peran penting pemangku kepentingan dalam implementasi e-government. Temuan mereka menunjukkan bahwa keberhasilan sistem layanan digital publik sangat bergantung pada partisipasi aktif pemangku kepentingan dalam mendukung regulasi dan kebijakan keamanan. Sebaliknya, penelitian ini menemukan bahwa di Indonesia, keterlibatan pemangku kepentingan sering kali bersifat reaktif daripada proaktif, yang menyebabkan lambatnya adopsi strategi keamanan yang lebih menyeluruh. Hal ini tercermin dalam minimnya audit dan evaluasi terhadap regulasi seperti Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE, yang belum sepenuhnya diterapkan secara konsisten (Presiden Republik Indonesia, 2018). Penelitian ini juga mendukung temuan Luna-Reyes *dkk*. (2021), yang menyatakan bahwa kegagalan proyek digital pemerintah sering kali disebabkan oleh faktor nonteknis, termasuk kelemahan dalam jaringan organisasi dan manajemen. Namun, dibandingkan dengan penelitian Luna-Reyes yang lebih bersifat global, penelitian ini memberikan analisis spesifik terhadap insiden PDN, termasuk dugaan penyelewengan anggaran dan keterlibatan oknum internal (Clinten & Pertiwi, 2024). Dengan demikian, penelitian ini menawarkan perspektif yang lebih kontekstual untuk wilayah Indonesia. Dari segi teknologi, penelitian ini memperkuat argumen Handri *dkk*. (2023), yang menyoroti pentingnya penerapan standar seperti NIST dalam pengelolaan keamanan siber e-government. Handri *dkk*. mengemukakan bahwa kerangka kerja berbasis teknologi yang terintegrasi dapat meminimalkan risiko serangan siber. Penelitian ini melangkah lebih jauh dengan merekomendasikan penggunaan teknologi berbasis ML dan AI untuk mendukung deteksi dini ancaman, di samping penguatan pada elemen proses seperti peningkatan alokasi anggaran keamanan dan audit regulasi yang berkelanjutan.

E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1210

Penelitian ini tidak hanya mengonfirmasi temuan-temuan sebelumnya, tetapi juga memberikan konteks lokal yang lebih mendalam terkait kelemahan sistem keamanan siber di Indonesia. Integrasi antara budaya organisasi, regulasi yang kuat, literasi digital, dan teknologi canggih menjadi kunci untuk mengatasi kelemahan yang diidentifikasi. Dengan pendekatan ini, sistem keamanan siber pada proyek telematika di Indonesia dapat dirancang menjadi lebih tangguh, baik dalam menghadapi ancaman global maupun melindungi data sensitif masyarakat.

4. Kesimpulan

Dalam Penelitian ini telah dilakukan eksplorasi kerangka kerja PPT sebagai strategi manajemen keamanan siber untuk proyek telematika SPBE di Indonesia dengan studi kasus kebocoran PDN. Metode eksplorasi dalam kajian ini mengidentifikasi faktor-faktor penyebab insiden siber PDN dan memetakannya ke dalam kerangka kerja PPT untuk mengklasifikasikannya berdasarkan aspek manusia, proses, dan teknologi, sehingga memudahkan dalam menentukan solusi penanganannya. Hasil identifikasi dan pemetaan penyebab insiden siber pada PDN ke dalam kerangka kerja PPT menunjukkan bahwa terdapat sebanyak 3 faktor manusia, 4 faktor proses, dan 7 faktor teknologi. Strategi manajemen keamanan siber untuk proyek telematika di Indonesia yang diusulkan dalam kajian ini berupa solusi-solusi penanganan, mitigasi, dan antisipasi insiden siber sesuai dengan kerangka kerja PPT yang berdasarkan pada studi kasus yang dipelajari dalam kajian ini. Para penyelenggara atau manajer proyek telematika di Indonesia dapat mengacu dan menggunakan strategi manajemen keamanan siber yang telah dibahas dalam kajian ini untuk proyek telematika yang akan atau sedang dikembangkan dan atau dikelolanya guna terwujudnya aspek keamanan siber dalam proyek telematika seperti SPBE. Pekerjaan di masa depan berdasarkan hasil kajian stratejik manajemen keamanan siber terhadap proyek telematika yang telah dikaji dalam makalah ilmiah ini adalah menerapkan dan strategi manajemen keamanan siber yang diusulkan pada proyek telematika dan membuat kerangka kerja strategi keamanan siber khusus proyek telematika.

5. Daftar Pustaka

Adristi, F. I., & Ramadhani, E. (2024). Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede. *Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen*, *2*(6), 196-212.

Al Ihsan, R., & Sekti, B. A. (2024). Pentingnya Keamanan Data Dalam Era Digital: Refleksi Terhadap Serangan Hacker Pada Pusat Data Nasional Indonesia. *Prosiding SISFOTEK*, *8*(1), 7-11.

Ashaye, O. R., & Irani, Z. (2019). The role of stakeholders in the effective use of e-government resources in public services. *International Journal of Information Management*, *49*, 253-270. https://doi.org/10.1016/J.IJINFOMGT.2019.05.016.

CNN Indonesia. (2024, Juni 28). Fakta-fakta Kebocoran Data PDNS, Dalang hingga Jumlah Tebusan. *CNN Indonesia*. https://www.cnnindonesia.com/teknologi/20240624122531-185-1113359/fakta-fakta-kebocoran-data-pdns-dalang-hingga-jumlah-tebusan.

Edgar, T. W., & Manz, D. O. (2017). *Research methods for cyber security*. Syngress.

E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1210

Ferdynandus, F., Prihanto, J. N., & Winarno, W. (2024). Implementing NIST Framework and the People, Process, Technology approach in Indonesian Financial Services. *International Journal of Engineering Continuity*, *3*(1), 172-182. https://doi.org/10.58291/IJEC.V3I1.265.

Ghaffari, F., Gharaee, H., & Arabsorkhi, A. (2019, April). Cloud security issues based on people, process and technology model: A survey. In *2019 5th International Conference on web research (ICWR)* (pp. 196-202). IEEE. https://doi.org/10.1109/ICWR.2019.8765295.

Güler, M., & Büyüközkan, G. (2023). A survey of digital government: Science mapping approach, application areas, and future directions. *Systems*, *11*(12), 563. https://doi.org/10.3390/SYSTEMS11120563.

Handri, E. Y., Putro, P. A. W., & Sensuse, D. I. (2023, August). Evaluating the People, Process, and Technology Priorities for NIST Cybersecurity Framework Implementation in E-Government. In *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)* (pp. 82-87). IEEE. https://doi.org/10.1109/ICOCICS58778.2023.10277024.

Ibrahim, A., Arief, A., & Do Abdullah, S. (2020). Keamanan Untuk Penerapan Layanan Publik Pada Sistem Pemerintahan Berbasis Elektronik (Spbe): Sebuah Kajian Pustaka Sistematis. *IJIS-Indonesian Journal On Information System*, *5*(2), 135-143. https://doi.org/10.36549/IJIS.V5I2.105.

Indonesia, P. (2018). Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. *Lembaran Negara Republik Indonesia*.

Jou, Y. T., Mariñas, K. A., Saflor, C. S., Baleña, A., Gutierrez, C. J., Dela Fuente, G., ... & Young, M. N. (2024). Investigating Various Factors Influencing the Accessibility of Digital Government with eGov PH Mobile Application. *Sustainability*, *16*(3), 992. https://doi.org/10.3390/SU16030992.

Khoerunisa, D. (2024). Analisis Framing Model Robert N. Etnman Pada Pemberitaan Kebocoran Pusat Data Nasional (PDN) di Media Online. *IKRA-ITH HUMANIORA: Jurnal Sosial dan Humaniora*, *8*(3), 153-162.

Luna-Reyes, L. F., Andersen, D. F., Black, L. J., & Pardo, T. A. (2021). Sensemaking and social processes in digital government projects. *Government Information Quarterly*, *38*(2), 101570. https://doi.org/10.1016/J.GIQ.2021.101570.

Medaglia, R., Misuraca, G., & Aquaro, V. (2021, June). Digital government and the united nations' sustainable development goals: towards an analytical framework. In *DG. O2021: The 22nd annual international conference on digital government research* (pp. 473-478). https://doi.org/10.1145/3463677.3463736.

Rahman, F. (2021). Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia. *Jurnal Legislasi Indonesia*, *18*(1), 81-102.

Ramadhani, E. H., & Wulandari, A. (2024, September). Studi Eksplorasi dan Desain Software Defined Network (SDN) untuk Jaringan Internet of Things (IoT) pada Smart Campus Studi Kasus di Kampus Politeknik Negeri Jakarta (PNJ). In *Seminar Nasional Teknik Elektro* (Vol. 10, No. 1, pp. 1-8).

E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1210

Ramadhani, E. H., Suyitno, D., & Suryantoro, S. (2024, February). Information technology security assessment (ITSA) methodology for web-based E-government. In *AIP Conference Proceedings* (Vol. 2838, No. 1). AIP Publishing. https://doi.org/10.1063/5.0179775/3267183.

Ramdhan, T. W., Florina, I. D., & Permadi, D. (2024). Analisis Framing Pemberitaan Peretasan Pusat Data Nasional (PDN) di Media Online Tempo. co. *Journal of Education Research*, *5*(3), 3368-3379. https://doi.org/10.37985/JER.V5I3.1491.

Sapraz, M., & Han, S. (2024). Users' evaluation of a digital government collaborative platform (DGCP) in Sri Lanka. *Transforming Government: People, Process and Policy*, *18*(1), 131-144.

Scholl, H. J. (2020). Digital government: looking back and ahead on a fascinating domain of research and practice. *Digital Government: Research and Practice*, *1*(1), 1-12. https://doi.org/10.1145/3352682.

Siber, B. (2021). Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik. *Bssn. Go. Id.*

Skierka, I. (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis. *Government Information Quarterly*, *40*(1), 101781.

Taherdoost, H. (2022). Cybersecurity vs. information security. *Procedia Computer Science*, *215*, 483-487. https://doi.org/10.1016/J.PROCS.2022.12.050.

Xue, Y., Chen, L., Feng, Z., & Huang, Y. (2024). Breaking the resource curse: Heterogeneous effects of digital government. *Resources Policy*, *90*, 104828. https://doi.org/10.1016/J.RESOURPOL.2024.104828.