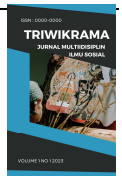
Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6, 2025
E-ISSN: 2988-1986
Open Access:



KESENJANGAN KAPABILITAS KEAMANAN SIBER INDONESIA DALAM MITIGASI SERANGAN SIBER PADA LAYANAN PUBLIK DIGITAL TAHUN 2020-2025

Asy Syuraya Arba Ilaina[1], Imam Fadhil Nugraha[2]
[1,2] Departemen Ilmu Hubungan Internasional,
Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin

ARTICLE INFO

Article history:
Received May, 2025
Revised May, 2025
Accepted May, 2025
Available online May, 2025

syurayauya@gmail.com,
Imamfadhil86@gmail.com

A B S T R A K

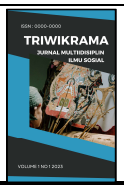
Dalam lima tahun terakhir Indonesia menghadapi peningkatan yang signifikan dalam jumlah dan kompleksitas serangan siber yang terjadi, mulai dari pencurian data sampai dengan peretasan infrastruktur digital. Tulisan ini menelaah bagaimana negara merespons tantangan yang terjadi melalui lensa *resilience governance*-pendekatan yang menekankan mengenai pentingnya fleksibilitas, adaptasi, dan keberlanjutan sistem yang ada dalam menghadapi risiko dunia modern. Dengan menggunakan metode penulisan kualitatif deskriptif dan menganalisis berbagai laporan insiden, kebijakan nasional, dan tata kelola pusat juga daerah. Tulisan ini menemukan bahwa respon Indonesia saat ini masih reaktif dan belum sepenuhnya mengadopsi prinsip-prinsip pertahanan jangka panjang. Beberapa tantangan utama yang diidentifikasi: belum optimalnya sistem deteksi dini kejahatan siber, koordinasi antara pemerintah pusat dan daerah yang lemah, serta ketergantungan Indonesia terhadap teknologi asing tanpa cadangan sistem nasional. Selain itu, perbandingan antara pendekatan keamanan siber pada era Jokowi dengan proyeksi tujuan kedepan untuk kebijakan di bawah Prabowo yang menunjukkan adanya potensi pergeseran fokus dari digitalisasi menuju pendekatan militeristik sembari menerapkan efisiensi anggaran. Temuan tersebut menggarisbawahi kebutuhan yang mendesak akan reformasi kebijakan dalam sektor keamanan siber yang tak hanya bersifat teknis, tapi juga memperkuat tata kelola yang adaptif dan kolaboratif terhadap risiko ancaman digital di masa depan.

Kata Kunci*:* Keamanan Siber; *Resilience Governance*; Serangan Siber; Tata Kelola; Indonesia.

A B S T R A C T

In the last five years Indonesia has seen a significant increase in the number and complexity of cyberattacks, ranging from data theft to hacking of digital infrastructure. This paper examines how the country has responded to these challenges through the lens of resilience governance-an approach that emphasizes the importance of flexibility, adaptability, and sustainability of existing systems in the face of risks in the modern world. Using descriptive qualitative writing methods and analyzing various incident reports, national policies, and central and local governance. This paper finds that Indonesia's current response is still reactive and has not fully adopted long-term defense principles. Several key challenges were identified: cybercrime early detection systems are not yet optimal, coordination between central and local governments is weak, and Indonesia's reliance on foreign technology without a backup national system. Moreover, a comparison between the cybersecurity approach under Jokowi and the projected future policy objectives under Prabowo that shows a potential shift in focus digitalization towards a militaristic approach while implementing budget efficiency. These findings underscore

*Corresponding author
E-mail addresses: syurayauya@gmail.com



the urgent need for policy reforms in the cybersecurity sector that are not only technical in nature, but also strengthen adaptive and collaborative governance against future digital threat risks.
***Keywords**: Cybersecurity; Resilience Governance; Cyberattacks; Governance; Indonesia.*

1. PENDAHULUAN

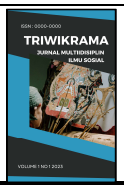
Di tengah kemajuan teknologi digital yang menjadi penanda kemajuan bangsa, sistem keamanan kita justru menjadi runtuh karena serangan yang tidak terlihat. Saat layanan publik berpindah ke ranah digital demi transparansi dan efektivitas, kita malah melihat sistem yang dibentuk untuk melayani publik justru menjadi sasaran kriminal siber. Transformasi digital sudah menjadi prioritas utama pembangunan nasional dari Indonesia dalam beberapa tahun belakang. Pemerintah melalui beberapa program misalnya Sistem Pemerintahan Berbasis Elektronik (SPBE) dan digitalisasi pada layanan publik menjadikan penggunaan teknologi sebagai bentuk keterbukaan dan keefektifan. Namun demikian, di balik kemajuan itu terdapat ancaman yang malah menunggangi kerentanan digital sebagai titik serang. Ancaman yang paling signifikan pada era ini adalah serangan siber, yang terus meningkat baik itu dari segi keragaman maupun intensitasnya.

Berdasarkan laporan dari Yudhi Kukuh saat memaparkan Laporan Keamanan Siber di Indonesia, bahwa sepanjang enam bulan pertama tahun 2024, Indonesia mendapat 2,49 miliar serangan siber, atau dapat dikatakan naik sebanyak enam kali lipat dibanding periode tahun sebelumnya. Mayoritas serangan siber ini bersumber dari dalam negeri yang menunjukkan bahwa potensi ancaman bukan hanya dari eksternal, melainkan juga berasal dari dalam sistem sendiri (Fikrie, 2024). Peristiwa peretasan yang menargetkan PT. Kereta Api Indonesia (KAI), Badan Siber dan Sandi Negara (BSSN), juga kebocoran data dari lembaga pendidikan dan badan transportasi menyatakan bahwa sektor layanan publik digital memang menjadi sasaran empuk (Aswara, 2024). Pada tahun 2021, data sekitar 279 juta warga Indonesia termasuk yang sudah meninggal dunia, diduga diretas dan diperjualkan dalam forum daring. Data tersebut diduga berasal dari Badan Penyelenggara Layanan Kesehatan (BPJS) dan pada Mei 2021, data kependudukan yang diduga bersumber dari Komisi Pemilihan Umum (KPU) sebanyak 2,3 juta WNI yang terdapat nomor induk kependudukan (NIK) serta nama dan alamat lengkap diduga bocor dan dibagikan dalam forum komunitas hacker (Amindoni, 2021).

Ancaman tersebut membuktikan pentingnya keamanan siber dalam hal transformasi digital nasional Indonesia. Dalam lingkup publik yang terus terdigitalisasi, kepercayaan masyarakat kepada layanan digital dipengaruhi dengan sejauh mana keamanan data dan transaksi dikelola. Jika sistem tidak dapat bertahan dan merespon dengan cepat saat ada serangan, hal tersebut tidak hanya akan berdampak teknis melainkan juga sosial. Kebocoran data pribadi, terganggunya layanan publik, sampai dengan hilangnya legitimasi pemerintah di mata publik. Kepercayaan digital atau keyakinan pengguna layanan terhadap sistem digital termasuk di dalamnya keamanan juga privasi serta keandalan merupakan hal fundamental untuk membangun hubungan yang kuat antara penyedia dan pengguna layanan digital. Kepercayaan masyarakat terhadap pemerintah tumbuh dari pelayanan publik yang baik, transparan, dan adanya partisipasi publik dalam penyusunan kebijakan (Nestitie, 2025).

Untuk memahami dinamika yang cukup kompleks, tulisan ini menggunakan dua teori: *Risk Society* dari Ulrich Beck dan *Resilience Governance*. *Risk Society* menjelaskan bagaimana risiko baru yang terbentuk oleh modernisasi, termasuk di dalamnya resiko teknologi dan cara publik serta negara perlu beradaptasi dalam pengelolaannya. Di sisi lain, teori *Resilience Governance* memandang penting sistem tata kelola yang tak hanya mencegah, akan tetapi juga mampu beradaptasi dan pulih dari masalah atau gangguan.

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:

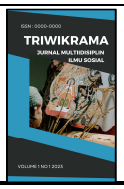


Masalah utama dalam tulisan ini adalah kapabilitas keamanan siber Indonesia yang masih timpang dan strategi mitigasi resilien yang dapat dibentuk dalam menghadapi ancaman terhadap layanan publik digital. Masalah ini mencerminkan kebutuhan untuk menelaah yang tidak hanya teknis, melainkan juga ketimpangan struktural dalam tatanan keamanan siber di Indonesia. Tulisan ini akan menyoroti kesenjangan koordinasi antara daerah dan pusat, ketergantungan pada industri asing, serta lemahnya pendeteksi dan respon cepat tanggap Indonesia terhadap kasus siber. Oleh karena itu, tujuan dari tulisan ini adalah untuk menganalisis kesenjangan kapabilitas keamanan siber Indonesia pada periode 2020-2025 dan merumuskan strategi mitigasi yang sesuai dengan prinsip *Resilience Governance* karena meningkatnya angka serangan siber yang tidak seimbang dengan peningkatan kesiagaan sistem keamanan digital Indonesia. Topik ini penting karena terdapat keamanan data publik, kepercayaan publik terhadap negara, dan kedaulatan negara di era digital. Tulisan ini akan menjelajahi beberapa isu utama: serangan siber selama pemerintahan Presiden Jokowi, kedepan mengenai prediksi arah kebijakan keamanan siber untuk era Prabowo serta ketergantungan kepada teknologi asing hingga akhirnya merumuskan rekomendasi mitigasi yang efektif.

2. TINJAUAN PUSTAKA

Transformasi digital yang menjadi pondasi modernisasi pelayanan publik telah menimbulkan kontradiksi bahwa semakin canggih dan terhubung sebuah sistem, maka akan semakin besar juga kerentanannya. Dalam hal ini, keamanan siber menjadi aspek yang krusial dan tak dapat diabaikan. Untuk mengetahui lebih lanjut mengenai bagaimana Indonesia menghadapi tantangan ini, dua pendekatan teoritik yaitu *Risk Society* dari Ulrich Beck dan *Resilience Governance* akan menjadi relevan untuk memahami situasi tersebut. Beck mengatakan bahwa modernisasi menghadirkan banyak risiko baru yang bersifat kompleks, termasuk di dalamnya risiko teknologi digital yang tak dapat diatasi dengan mekanisme tradisional. Serangan siber adalah bentuk nyata dari *manufactured risks*-risiko yang dibuat oleh sistem modern itu sendiri (Kusvianti, Ashari, & Izzah, 2023). Indonesia tidak hanya menjadi korban serangan dari luar, akan tetapi juga berhadapan dengan potensi bahaya yang bersumber dari lemahnya pertahanan internal yaitu ketimpangan infrastruktur digital, birokrasi yang lambat, dan dependensi pada teknologi asing. Kemandirian bangsa tidak akan optimal jika pemerintah masih memiliki ketergantungan yang besar terhadap industri siber luar negeri.

Dalam menghadapi situasi seperti ini, memperkuat sistem keamanan belum cukup. Indonesia membutuhkan pendekatan yang menyeluruh dan tahan banting. Oleh sebab itu, konsep Resilience Governance penting dalam hal ini. Konsep ini menekankan bahwa sistem kelembagaan dan pemerintahan harus dirancang tak hanya untuk mencegah serangan, melainkan juga untuk cepat pulih, beradaptasi, dan belajar dari gangguan yang telah terjadi. Negara tetangga Indonesia, Singapura telah lebih dulu menerapkan pendekatan ini dalam membangun sistem keamanan siber yang tangguh. Meskipun masih menjadi target serangan siber, Singapura termasuk sebagai negara dengan kesiapan ketahanan siber yang mumpuni (Putra K. I., 2019, p. 2). Dengan menggunakan kedua teori tersebut, dapat di identifikasi bahwa persoalan siber di Indonesia bukan hanya tentang teknologi, tapi juga mengenai cara negara mengelola risiko dan membangun pertahanan. Kelemahan utama sistem keamanan siber pemerintah adalah kurangnya investasi dalam teknologi dan pelatihannya (Zulfikar, 2024). Banyak instansi yang masih menggunakan perangkat lunak maupun perangkat keras yang telah usang dan tidak lagi didukung dengan keamanan terbaru. Perangkat lunak yang tidak diperbarui mengakibatkan lemahnya keamanan pada perangkat yang membuat sistem mudah diretas (Singgih, 2025).



3. METODE

Tulisan ini menggunakan pendekatan kualitatif untuk memahami ancaman siber transnasional mempengaruhi ketahanan nasional Indonesia. Fokus utamanya adalah melihat respon negara terhadap ancaman yang muncul, dari sisi kebijakan, strategi keamanan, sampai kerangka kerja institusional yang ada. Data dalam tulisan ini diperoleh melalui studi kepustakaan yang menggunakan berbagai sumber tertulis seperti jurnal ilmiah, laporan lembaga nasional maupun internasional, serta dokumen resmi dari pemerintahan. Sumber ini dipilih karena relevan untuk menjelaskan konsep dan bentuk ancaman siber di Indonesia, pertahanan nasional dalam lingkup siber, dan kaitannya dengan keamanan non-tradisional di Indonesia. Proses pengumpulan data dilakukan dengan mengeksplor literatur yang relevan dengan topik melalui database akademik dan publikasi yang terpercaya. Data yang telah dikumpulkan kemudian dianalisis secara deskriptif untuk menemukan pola, kecenderungan, dan narasi yang muncul dalam keamanan digital tingkat nasional dan global. Analisis ini dilakukan untuk memperoleh pemahaman yang lebih dalam mengenai peran aktor negara dan non-negara dalam menangani isu keamanan siber serta strategi Indonesia dalam merespon tantangan tersebut. Hasil analisis tersebut kemudian akan dijadikan dasar dalam menyusun pembahasan dan menarik kesimpulan di akhir tulisan ini.

4. HASIL DAN PEMBAHASAN

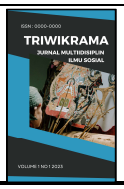
Permasalahan keamanan siber yang ada di Indonesia tak hanya mencerminkan tingginya angka ancaman digital, melainkan juga memperlihatkan lemahnya kesiapan sistem dalam merespon berbagai insiden yang terjadi. Kajian teoritis sebelumnya telah menekankan mengenai pentingnya pendekatan resilience governance sebagai kerangka konseptual untuk menilai dan membimbing arah kebijakan keamanan siber, bukan hanya dari proteksi secara teknis, tetapi juga kemampuan adaptasi, koordinasi, dan keberlanjutan sistem guna menghadapi krisis yang seringkali tak terduga. Dengan pendekatan tersebut, pembahasan ini tak hanya menjelaskan situasi yang ada saat ini, tapi juga memberi gambaran yang utuh mengenai tantangan dan peluang untuk perbaikan tatat kelola keamanan siber Indonesia kedepannya.

4.1 Bentuk Serangan Siber dan Kapasitas Respon Indonesia (2020-2024)

Dalam lima tahun belakangan, kasus siber di Indonesia terus terjadi dan meningkat. Serangan ini tidak hanya menargetkan lembaga pemerintahan, melainkan juga sektor-sektor swasta, layanan transportasi, hingga layanan publik seperti sistem pendidikan dan rumah sakit. Badan Siber dan Sandi Negara (BSSN) mencatat serangan siber tahun 2020 mencapai angka 495,3 juta atau meningkat 41 persen dari tahun sebelumnya. Dimana pada tahun 2019 terhitung 4.586 laporan polisi melalui laman web Bareskrim melaporkan kejahatan siber meningkat angkanya dari tahun sebelumnya pada 2018. (Christianingrum & Aida, 2021). Sama halnya dengan Badan Reserse Kriminal Kepolisian Negara Republik Indonesia (Bareskrim), melihat bahwa terdapat peningkatan laporan kejahatan siber. Indonesia mengalami rata-rata 13 juta serangan siber perhari, atau 158 serangan siber per detik (Fikrie, 2024). Kita lihat ada peningkatan serangan siber di Indonesia dan cukup signifikan. Serangan itu meningkat sebanyak lebih dari 600 persen, menurut laporan (Zamzama, 2024).

Jenis serangan yang seringkali terjadi yaitu peretasan situs, penyebaran *malware*, pencurian data pribadi hingga *Distributed Denial of Service* (DdoS) yaitu serangan siber yang membuat sistem atau layanan tidak tersedia bagi pengguna yang asli dengan cara memenuhi sistem tersebut dengan lalu lintas internet yang besar. Salah satu kasus serangan siber yang sempat ramai dibicarakan pada Juni 2024 lalu yaitu server Pusat Data Nasional

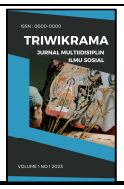
Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:



(PDN) yang terkena serangan berupa perangkat lunak berbahaya oleh group *Brain Cipher*. Terdapat 282 instansi pemerintah yang mencakup data kementrian dan lembaga, serta pemerintah provinsi, kabupaten, dan kota (Lavenia, 2024). Mereka beraksi dan meminta uang tebusan sebesar 131,8 miliar rupiah untuk membuka gembok pada data-data fasilitas itu (Aswara, 2024). Imbas dari serangan siber tersebut adalah lebih dari 200 layanan instansi pemerintas terganggu. Dalam hal ini, berimbas paling besar kepada layanan imigrasi termasuk aplikasi paspor dan visa yang lumpuh. Menteri Hukum dan HAM mengatakan pihaknya terpaksa memindahkan layanan imigrasi ke *Amazon Web Services*. Setelah lima hari akhirnya lewat keterangan resmi, Direktur Jenderal Imigrasi, Silmy Karim, menjelaskan bahwa sistem aplikasi sudah kembali normal. Selain Kementrian Hukum dan HAM, instansi lain juga ikut terdampak yaitu Kementrian Koordinator Bidang Kemaritiman dan Investasi, Kementrian PUPR, LKPP sampai Pemerintah Daerah Kediri (BBC, 2024). Pada November 2023, terdapat 204 juta data Pemilu 2024 dibobol dari situs Komisi Pemilihan Umum (KPU), oleh akun anonim "Jimbo". Sebelumnya pada Juli 2023 akun "Bjorka" membocorkan 34 juta data paspor WNI, lalu pada bulan yang sama, 337 juta data Dukcapil Kementrian Dalam Negeri dibobol oleh peretas dengan nama "RRR" (Kansong, 2024).

Pusat data pemerintah masih rentan karena kurangnya keseriusan dari Kominfo dan BSSN dalam menangani serangan siber. Kedua lembaga tersebut selalu mengalami kesulitan dan kebingungan ketika terjadi serangan siber yang menyerang data pemerintah. Hal itu membuktikan belum ada tindakan penegakan yang serius dilakukan untuk menangani kerentanan sistem data pemerintah padahal imbas dari kebocoran data pemerintah ini akan ada tiga kemungkinan penyalahgunaan data yang dapat membahayakan masyarakat, seperti penipuan terstruktur, penyalahgunaan identitas dan judi online. Sementara pemerintah terjebak dalam posisi serba salah akibat serangan siber. Sebab, jika pemerintah memilih untuk tidak membayar tebusan yang diminta, terdapat risiko data yang diretas akan hilang total atau bahkan dibocorkan ke dunia maya. Selain itu, pemerintah mesti memulihkan data itu dengan sendirinya dalam waktu yang singkat sedangkan membuka data itu sendiri membutuhkan waktu yang sangat lama. Namun, jika pemerintah memilih untuk membayar tebusan kepada pelaku, maka Indonesia akan dipandang sebagai negara yang mudah diperas dan rentan terhadap serangan siber dan akan memposisikan Indonesia sebagai sasaran yang empuk untuk diserang. Lagipula, ada beberapa kasus pihak peretas menerima uang tebusan namun tidak memulihkan data yang telah dijanjikan di awal (Wijaya, 2024). Maka dari itu, pemerintah tidak akan membayar uang tebusan yang menjadi permintaan pihak peretas, melainkan meminta polisi untuk mengusut pelanggaran pidana tersebut. Data yang diretas di coba untuk dipulihkan secepat dan sebanyak mungkin sembari Kemenkominfo berupaya memitigasi risiko terkena serangan siber dengan membangun pusat data nasional lebih permanen di tiga titik, yaitu di Batam, Cikarang dan IKN. Kemenkominfo juga merancang desain perlindungan data yang disertai tes penetrasi serangan berkala (Yanuar, 2024).

Masalah lain yang juga ada yaitu belum maksimalnya kemampuan sistem peringatan dini sehingga serangan baru bisa terdeteksi ketika sudah besar. Hal ini menunjukkan bahwa Indonesia masih lemah dalam hal mendeteksi dan mencegah serangan sejak dini. Dalam menghadapi risiko keamanan, deteksi dini adalah kunci. Sistem keamanan yang dapat mendeteksi hal mencurigakan atau pola yang tidak seperti biasanya dalam waktu yang nyata bisa mengurangi dampak serangan yang signifikan. Memajukan kapabilitas pendeteksian dini melibatkan investasi seperti teknologi yang canggih, pelatihan yang lebih baik kepada tenaga kerja, serta implementasi praktik keamanan yang diawasi dengan ketat (Teknokrat, 2025) sedangkan Indonesia masih mengalami banyak kekurangan alat pendeteksi dini dalam sektor siber. Sistem pendeteksian dini terhadap serangan siber yang



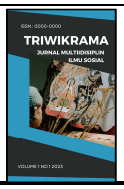
Indonesia miliki masih tertinggal dibandingkan negara-negara lain. Taiwan misalnya, memiliki enam ribu sensor pendeteksi dini, sedangkan Indonesia hanya mempunyai 21 sensor yang tersebar di enam provinsi (Lim, 2019). Tentu minimnya jumlah sensor deteksi ini disebabkan karena anggaran yang terbatas untuk menyediakan sensor karena jika pemerintah memprioritaskan keamanan siber, maka pasti akan ada alokasi dana dan teknologi yang mumpuni. Padahal pada kenyataannya keamanan siber juga merupakan hal yang krusial dan juga perlu untuk di prioritaskan.

Di sisi lain, Indonesia juga menghadapi tantangan mengenai sumber daya manusia dan ketergantungan pada teknologi asing. Terdapat banyak lembaga yang masih kekurangan tenaga profesional dalam keamanan siber, sembilan dari 10 lulusan teknologi lebih memilih menjadi developer perangkat lunak, bukan bekerja dalam keamanan dan proteksi siber. Saat ini hanya ada sekitar 10 dari total 4.000 kampus di Indonesia yang menyediakan jurusan keamanan siber. Hal tersebut yang membuat banyak perusahaan merekrut ahli keamanan siber yang berasal dari negara lain (Herman, 2022). Jika dilihat secara keseluruhan, kondisi tersebut menunjukkan bahwa Indonesia masih berada dalam tahap membangun keamanan siber dan membutuhkan perhatian yang lebih. Pendekatan yang digunakan selama ini masih lebih fokus pada penanganan darurat, bukan pencegahan jangka panjang. Penanganan baru akan dilakukan setelah serangan muncul, berarti bahwa ancaman baru yang belum pernah terjadi bisa terus lolos (Sari, 2024). Hal ini yang membuktikan bahwa dalam keamanan siber, Indonesia masih bersikap reaktif bukan proaktif yang berarti hanya ditindak setelah ancaman terdeteksi, bukan malah mencegahnya. Fenomena seperti itu menunjukkan karakteristik *risk society* dari Beck, yang mana teknologi justru menjadi sumber risiko sistemik yang baru. Kondisi dimana negara beradaptasi dengan lambat dan gagal membangun kapasitas prediktif, maka risiko-risiko digital justru diperbesar dengan struktur institusional yang tidak lentur. Disisi lain melalui *resilience governance*, Indonesia belum menunjukkan adanya fleksibilitas dan kapasitas yang cukup memadai, utamanya dalam hal merespon dan memprediksikan serangan.

4.2 Ketimpangan Tata Kelola dan Ketergantungan terhadap Teknologi Asing

Salah satu masalah yang mendasar dalam sistem tata kelola keamanan siber di Indonesia adalah adanya ketimpangan antara pusat dan daerah. Sampai saat ini, koordinasi yang harusnya menjadi pilar yang kuat justru masih sangat lemah. Pemerintah pusat pada kenyataannya telah meluncurkan berbagai kebijakan dan inisiatif digitalisasi. Kendati demikian, implementasi yang ada di sektor daerah seringkali tidak seragam. Banyak pemerintah daerah yang belum mempunyai unit khusus dan sumber daya manusia yang mampu menangani insiden siber secara profesional. Dari indikator keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE) tercatat terdapat 100 pemerintah daerah yang belum memiliki kebijakan manajemen keamanan. Sebanyak 300 pemerintah daerah belum kunjung menerapkan kebijakan keamanan, serta sekitar 450 pemerintah daerah belum kunjung melaksanakan audit keamanan SPBE tersebut (Diskominfo, 2024). Di sisi lain, pasukan TNI yang masih minim juga turut menjadi masalah keamanan siber di Indonesia. Komandan Pussansiad Brigjen TNI menerangkan bahwa jumlah personel Pusat Sandi dan Siber TNI AD hanya sekitar 130 orang, sementara ketentuan targetnya adalah 197 orang dan disampaikan bahwa angka itu masih belum memadai (Antara, 2021). Menanggapi hal ini, Pusat Sandi dan Siber TNI seharusnya merekrut lebih banyak ahli siber dari prajurit TNI guna keamanan yang lebih ketat. Diperlukan tenaga yang lebih banyak demi membangun kekuatan siber di Indonesia baik itu di pusat maupun daerah.

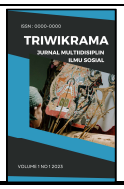
Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:



Minimnya kapasitas kelembagaan di tingkat daerah semakin memperburuk keadaan. Bukan hanya anggaran dan infrastruktur, tapi juga kesadaran akan pentingnya keamanan digital dan budaya organisasi di tingkat daerah. Hal ini menyebabkan banyaknya kasus kebocoran data dan gangguan sistem di daerah yang sulit untuk ditangani dengan baik atau bahkan tidak dilaporkan. Insiden peretasan situs pemerintah Pemalang yang memicu kekhawatiran publik, mengingat terus meningkatnya ancaman siber di Indonesia beberapa tahun belakang. Pemerintah setempat menjelaskan bahwa data yang bocor adalah data yang masih dalam tahap uji coba, bukan data resmi. Kendati demikian, masyarakat tetap mengalami ketakutan akan serangan yang bisa datang kapan saja (R, 2025). Walaupun data yang bocor dikatakan hanyalah data uji coba, kejadian tersebut tetap menjadi hal serius untuk keamanan sistem digital pemerintah. Kebocoran data sekecil apapun itu menunjukkan lemahnya perlindungan data pribadi publik di lingkup pemerintah Indonesia. Melihat banyaknya kasus kebocoran data, pemerintah daerah berperan besar dalam hal mengedukasi masyarakat mengenai pentingnya untuk melindungi data pribadi. Karena masyarakat juga perlu diedukasi tentang pengamanan informasi pribadi, termasuk di dalamnya menggunakan sandi yang kuat, tidak membagikan data sensitif sembarangan dan selalu waspada terhadap penipuan digital. Tingkat literasi digital di Indonesia hanya sebesar 62 persen dan jumlah tersebut paling rendah dibanding negara-negara di ASEAN yang menyentuh 70 persen (Anam, 2023). Oleh karena itu, diperlukan percepatan untuk mengajarkan literasi digital di Indonesia bagi semua kalangan. Hal tersebut butuh perhatian besar pemerintah guna mendorong masyarakat terhindar dari segala bentuk penipuan berbau teknologi yang bisa menghadapi era digital kedepan.

Dari sudut pandangan kelembagaannya, struktur tata kelola siber yang ada di Indonesia terpusat, di mana pusat memiliki legitimasi, dan sumber daya, sementara daerah hanya menjadi implementator tanpa adanya kontrol yang memadai. Melalui *resilience governance*, desentralisasi yang tidak berangkat dengan transfer kapasitas, hanya menimbulkan kerentanan keamanan, di mana titik rawan justru menjadi terkonsentrasi di wilayah tertentu yang miskin akan kapasitas.

Masalah lain yang juga tidak kalah serius adalah dependensi tinggi Indonesia terhadap teknologi luar negeri, utamanya dalam hal perangkat keras dan lunak, serta layanan keamanan sibernya. Saat ini, kebanyakan sistem keamanan digital yang digunakan oleh pemerintahan baik itu pusat maupun daerah, bergantung kepada vendor asing. Sayangnya, dominasi vendor asing seperti ini tidak seimbang dengan sistem cadangan nasional yang cukup memadai. Ketiadaan sistem redundasi seperti pusat data cadangan dan protokol krisis berbasis lokal merupakan permasalahan yang serius. Dalam berbagai kasus, terdapat banyak perangkat dari vendor asing yang bahkan pihak lokal tidak sepenuhnya bisa mengendalikannya, baik itu dari segi pemeliharaan maupun respon terhadap insiden. Hal tersebut yang membuat lembaga publik kerap kesulitan mengalihkan layanannya ke sistem darurat dikarenakan sistem yang tidak memadai. Jumlah pusat data lokal di Indonesia yang memenuhi standar International *Organization for Standardization* (ISO) yaitu 2.700 pusat data yang ada, namun hanya 3 persen yang memenuhi standar internasional (Aptika, 2020). Ketergantungan yang terdapat dalam berbagai sektor yang seharusnya menjadi evaluasi untuk pemerintah, salah satunya dalam sektor keamanan siber seperti inilah yang seharusnya Indonesia kurangi dan perlu di upayakan untuk menjadi lebih independen untuk mengatasinya. Untuk mengurangi ketergantungan Indonesia terhadap teknologi asing, pemerintah perlu meningkatkan investasinya lagi dalam sektor keamanan digitalnya. Karena secara keseluruhan dependensi Indonesia terhadap teknologi asing bisa memberikan dampak negatif pada pertahanan dan keamanan nasional nantinya (Prabowo & Sihaloho,



2023). Dalam *resilience governance*, ketergantungan Indonesia pada teknologi luar negeri juga ketidaksiapan sistem internal menunjukkan bahwa adaptivitas dan kontinuitas yang rendah. Indonesia belum memprioritaskan untuk meningkatkan kemampuan dan potensi SDM serta pemborosan sumber daya dan biaya dalam sektor lain.

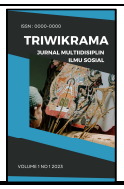
Di sisi lain, kapasitas sumber daya manusia dalam negeri yang belum mampu menjawab tantangan yang kompleks keamanan digital di Indonesia. Kurangnya pendidikan dan pelatihan teknis yang mendalam dan ekosistem pengembangan individu di bidang keamanan siber ini menyebabkan Indonesia bergantung banyak pada pihak luar. Masih kurangnya kesadaran mengenai karir dalam bidang keamanan siber yang menyebabkan tidak banyak individu yang memiliki ketertarikan untuk mengejar karir dalam bidang itu (Budin, 2024). Hal ini menunjukkan bahwa tak hanya teknologi yang di impor, tetapi juga pengetahuan dan keahlian dalam mengelola teknologinya. Tenaga profesional dalam bidang IT khususnya keamanan siber di Indonesia masih kurang banyak. Anggota yang Indonesia miliki hanya 1100 orang, sedangkan negara kecil seperti Singapura saja mempunyai 5500 orang (Ramadhan, 2024).

Jika ditinjau dari lensa teori *risk society*, situasi seperti ini membuktikan bagaimana risiko-risiko baru bermunculan akibat pilihan modernisasi merupakan langkah yang diambil secara tidak merata dan tidak berpijak pada penguatan kapasitas internal yang ada. Sebagaimana *risk society* menyatakan bahwa meningkatnya kompleksitas dan ketidakpastian masyarakat dunia modern karena adanya keterkaitan global, ancaman lingkungan dan kemajuan teknologi. Beck mengatakan bahwa masyarakat modern akan semakin dicirikan oleh berkembangnya risiko buatan mereka sendiri yang menentang batas kerangka kerja yang ada (Putra A. M., 2024). Pada kondisi saat ini keamanan digital yang seharusnya menjadi aspek yang perlu tumbuh beriringan bersama dengan transformasi digital, bukan malah menjadi beban tambahan. Namun pada kenyataannya, langkah untuk mempercepat proses digitalisasi tanpa membangun pengamanan justru menimbulkan banyak risiko baru yang dapat merugikan publik. Sementara itu, dari sudut pandang *resilience governance* memandang hal ini sebagai bentuk lemahnya sistem yang terintegrasi antara pusat dengan daerah juga dominasi teknologi luar negeri menunjukkan betapa kurangnya fleksibilitas, adaptivitas, dan kesinambungan dalam tata kelola siber di Indonesia. Tanpa adanya fleksibilitas dalam menghadapi ancaman, kemampuan adaptasi nasional, dan sistem yang terus beroperasi bahkan di tengah krisis, maka prinsip *resilience* hanyalah jargon semata. Tidak sejalan dengan yang teori ini inginkan yaitu kemampuan sistem dan komunitas masyarakat untuk melawan, beradaptasi, dan pulih dari dampak suatu bencana (Rachmania, 2021). Berbeda dengan Singapura yang telah menerapkan konsep *resilience governance* dalam keamanan layanan publik digitalnya yang terbukti lewat minimnya kasus serangan siber dan kebocoran data di Singapura. *The Singapore Computer Emergency Response Team* (SingCERT) telah dibentuk dan bekerja untuk membantu proses deteksi, resolusi, serta pencegahan insiden serangan siber terhadap Singapura (Putra K. I., 2019). Hal seperti ini perlu dijadikan pertimbangan besar bagi pemerintah Indonesia untuk diterapkan demi pertahanan dan keamanan serta demi menjaga kepercayaan dan kenyamanan masyarakatnya.

4.3 Isu Serangan Siber pada Tahun 2020-2025 di Indonesia dalam Perspektif *Resilience Governance*

Indonesia saat ini sedang berada pada fase kritis dalam menata sistem keamanan sibernya. Semakin tinggi angka digitalisasi pada sektor layanan publik, ekonomi sampai dengan pertahanan mengakibatkan serangan siber tidak lagi bersifat tidak menentu,

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:

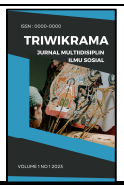


melainkan sistematis secara meluas. Dalam kurun waktu 2020 sampai dengan 2025, banyak serangan besar yang terjadi. Kebocoran data di BPJS Kesehatan, serangan terhadap situs milik KPU, hingga pembobolan aplikasi MyPertamina menjadi peristiwa serius yang menunjukkan bahwa kapasitas pertahanan siber nasional belum memadai di Indonesia. Pada tahun 2021 dibawah pemerintahan Presiden Jokowi, Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 1,6 miliar serangan siber terhadap Indonesia (Safitri, 2024). Pada masanya, kasus serangan siber utamanya kebocoran data pribadi bukan hanya terjadi satu kali, melainkan hal ini terus berulang. Kebocoran paling sering terjadi di instansi pemerintah, dimana pemerintah sendiri seakan tidak belajar dari masalah yang telah terjadi. Kebocoran data terbesar yaitu sebanyak 6 juta Nomor Pokok Wajib Pajak (NPWP) diperjualbelikan dengan harga 150 juta, data yang bocor pada saat itu adalah Nomor Induk Kependudukan, alamat, dan nomor kontak telepon seluler dan surat elektronik. Kasus kebocoran data lainnya seperti data 21 juta KTP dan paspor penumpang anak usaha Lion Air dan diunggah ke forum daring, data 230 ribu warga dalam kasus *Covid-19* yang dicuri peretas, sebanyak 2,3 juta data pribadi di situs web KPU juga ikut diretas, 279 juta data penduduk dari BPJS Kesehatan yang bocor, hacker yang menjual 44 juta data pengguna MyPertamina, kebocoran data 4,7 juta NIP dan NIK milik ASN, hingga puluhan ribu data polri yang diretas oleh peretas asal brasil dan masih banyak kasus besar lainnya (Yaputra, 2024).

4.3.1 Pendekatan Keamanan Siber Kepemimpinan Jokowi dan Proyeksi Prabowo

Dalam dua periode kepemimpinan Presiden Joko Widodo menempatkan transformasi digital sebagai salah satu sektor yang dijadikan prioritas nasional. Hal tersebut terlihat dari salah satu program pembangunan infrastruktur TIK untuk wilayah 3T (tertinggal, terdepan, dan terluar), dorongan besar terhadap ekonomi digital, serta digitalisasi layanan publik. DI bawah kepemimpinannya, Presiden Jokowi terus membangun dan memperkuat infrastruktur digital daerah 3T dengan tujuan pemerataan ini tidak hanya terpusat di suatu wilayah, melainkan membuka wilayah baru (Fauzi, 2023). Program Satu Data Indonesia, bentuk digitalisasi dalam sektor kesehatan melalui program PeduliLindungi dan sistem administrasi kependudukan berbasis digital. Akan tetapi, modernisasi seperti ini sering kali terfokus pada aspek teknologi dan kurang diimbangkannya proteksi siber yang memadai. Banyak institusi pemerintah yang telah menjalankan sistem digital, tetapi masih belum memiliki pertahanan yang kuat dalam menjalankannya. Kebocoran, manipulasi, hingga serangan yang menyebabkan kerugian finansial banyak sekali terjadi. Ditambah lagi, pelaku kejahatan siber kini makin terstruktur seperti layaknya sebiah entitas bisnis. Metode serangan yang semakin canggih sehingga bukan hanya mengancam keamanan data, melainkan juga berpotensi mengguncang stabilitas ekonomi nasional (Edavos, 2024).

Penanganan terhadap serangan siber pada masa pemerintahan Presiden Jokowi juga dapat dikatakan masih lemah dan belum cukup untuk dikatakan mumpuni dalam hal strategi mitigasi menghadapi kejahatan siber di Indonesia. Bukti bahwa lemahnya penanganan terhadap serangan siber dibuktikan langsung dengan kasus serangan yang terus bermunculan dan respon pemerintah yang kurang memuaskan masyarakat. Bahkan banyak kasus serangan siber yang membuat Kementrian Komunikasi dan Informatika (Kemkominfo), TNI, Polri yang justru tidak berkutik. Salah satu penyebab hal tersebut terjadi ialah dikarenakan pendekatan yang keliru oleh pemerintah dalam mengatasi serangan siber. Alih-alih mengedepankan kerja sama, pemerintah malah berniat membentuk angkatan siber untuk melengkapi tiga matra TNI, sementara membuat matra itu adalah konsep perang konvensional (Wahidin, 2024). Padahal pada



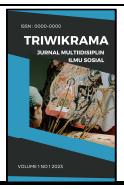
kenyataannya, siber tidak bisa hanya ditangani oleh matra TNI saja, Seharusnya pemerintah ikut menggandeng semua pihak yang berkecimpung dalam dunia siber guna merumuskan peta menuju sistem pertahanan siber yang mumpuni. Disamping itu, Indonesia juga belum memiliki UU Keamanan Siber yang memungkinkan BSSN untuk mempunyai kendali sepenuhnya untuk melakukan koordinasi secara efektif dan mengoptimalkan keamanan. BSSN sudah seringkali meminta agar UU ini menjadi prioritas dan dibentuk kembali, akan tetapi tidak bisa langsung meminta kepada DPR dikarenakan yang hanya bisa mengusulkan RUU ialah kementrian (Ina, 2024). Menanggapi hal ini, diperlukan adanya aturan yang tegas untuk memastikan kewenangan keamanan siber di Indonesia, demi menghindari adanya saling melempar tanggung jawab ketika keamanan siber diserang.

Sementara itu, meskipun pemerintahan Presiden Prabowo masih terhitung baru dimulai, fokus kebijakan yang diproyeksikan terlihat berbeda. Dalam berbagai kegiatan, seperti debat publik, dokumen visi-misi, pendekatan keamanan Prabowo terlihat lebih menekankan aspek pertahanan nasional juga efisiensi anggaran. Prabowo melihat bahwa dunia digital sebagai area baru peperangan dan karena itu, mendorong integrasi sistem siber ke dalam struktur militer dan intelijen yang lebih kuat merupakan suatu urgensi. Termasuk potensi pembentukan komando siber yang terkoordinasi langsung bersama dengan TNI serta peningkatan anggaran keamanan digital melalui pendekatan efisiensi dan sentralisasi. Prabowo dan Gibran berkomitmen untuk memperkuat pertahanan dan keamanan siber Indonesia melalui hirilisasi digital (Fitriana, 2024). Hal tersebut merupakan langkah penting dan antisipatif dalam merespon kejahatan siber yang mampu menjaga stabilitas nasional. Meskipun terdapat kecenderungan bahwa pendekatan keamanan siber akan lebih mengarah ke militer dan bersifat kontrol terpusat, akan tetapi langkah demikian tetap akan lebih baik dibandingkan harus menghadapi situasi dimana tanggung jawab suatu lembaga tidak menentu. Bentuk langkah kecil yang diberikan yaitu langkah nyata berupa pembelajaran mengenai keamanan siber pada tingkat perkuliahan.

Meskipun belum menentu, akan tetapi implikasi dari perbedaan pendekatan Jokowi dan Prabowo cukup signifikan jika dianalisa menggunakan perspektif *resilience governance*. Pendekatan Jokowi berisiko membangun sistem yang kuat secara infrastruktur akan tetapi lemah dalam kapasitas respon dan pemulihannya. Sementara pendekatan Prabowo berpotensi menciptakan sistem pertahanan siber yang kuat untuk di kontrol, namun mungkin saja akan mengkhawatirkan dalam hal inklusivitas, terlalu sentralistik, dan minim melibatkan masyarakat serta sektor swasta lainnya yang juga ikut terdampak serangan siber.

4.3.2 Evaluasi Melalui Resilience Governance

Tiga prinsip utama dalam konsep *resilience governance* adalah fleksibilitas, adaptivitas, dan kontinuitas. Ketiga hal tersebut merupakan landasan yang sangat penting dalam menciptakan sistem keamanan siber yang tak hanya defensif, tapi juga tangguh dalam melawan serangan yang terus terjadi dan tidak terduga. Dari segi fleksibilitas, respon antar lembaga terkesan masih kaku. Lembaga seperti Kominfo, BSSN, Kemenhan, dan institusi publik lain belum memperlihatkan koordinasi yang dinamis. Ketika terjadi insiden, informasi seringkali tidak transparan, koordinasi yang kurang baik, dan respon yang terhambat oleh birokrasi. Sedangkan dari segi adaptivitas, masih teradapat pekerjaan besar bagi Indonesia yang harus dibenahi. Serangan siber yang terus meningkat dan belum dibuat mekanisme yang efektif untuk memperbaharui kebijakan dan juga prosedur berdasarkan pengalaman dari peristiwa

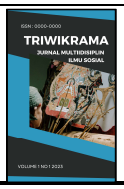


sebelumnya. Begitu banyak serangan yang tidak menghasilkan perubahan struktural yang signifikan, baik itu dari lembaga pemerintahan maupun sektor swasta. Sementara dalam hal kontinuitas layanan juga menjadi permasalahan yang cukup mencolok. Di saat serangan terjadi, layanan publik seketika lumpuh total tanpa adanya sistem pengembalian yang memadai untuk itu. Minimnya redundansi dan infrastruktur cadangan mengakibatkan waktu pemulihan mengambil waktu lama dan memberikan dampak sosial yang cukup signifikan, terutama dalam sektor layanan dasar seperti kesehatan, pendidikan, serta administrasi kependudukan. Masih banyak lembaga pemerintah dan swasta menjalankan sistem teknologi informasinya dengan standar keamanan yang belum cukup optimal. Terdapat beberapa institusi yang masih menggunakan sistem yang sudah usang dan penggunaan sandi lemah yang mengakibatkan rentan terhadap eksploitasi (Feradhita, 2025).

Strategi pemerintah yang selama ini berhasil dalam membangun peraturan hukum dan menyusun lembaga seperti pendirian BSSN, dan penyusunan regulasi mengenai keamanan data merupakan sebuah langkah awal yang penting. Namun, yang menjadi kelemahan utamanya adalah pengimplementasiannya dan kesenjangan kapasitas antar daerah. Tak semua daerah mempunyai SDM dan perangkat yang memadai untuk menjalankan sistem keamanan siber, sehingga terdapat ketimpangan dan membuka celah untuk serangan. Selain dari itu, pendekatan yang terlalu birokratis juga memperlambat respon terhadap suatu insiden yang terjadi. Padahal begitu banyak insiden penyerangan siber yang terjadi setiap harinya. Tantangan lain adalah kurangnya SDM yang spesifik dalam bidang forensik digital dan ahli digital serta belum ada pusat koordinasi insiden yang aktif 24 jam, juga ketidaktersediaan *backup* sistem yang tangguh dan kuat. *Resilience governance* tak hanya sekedar respon atas serangan dalam hal ini, melainkan transformasi melalui cara berpikir dan bertindak dalam menghadapi risiko yang kompleks. Negara masih ada dalam fase yang responsif saat ini, belum transformatif. Tanpa adanya perubahan pola berpikir yang menempatkan resiliensi sebagai fondasi penting dalam tata kelola digital, maka risiko akan selalu terjadi.

5. SIMPULAN DAN SARAN

Tulisan ini menemukan bahwa dalam kurun waktu 2020-2025, Indonesia menghadapi begitu banyak tantangan yang serius dalam keamanan siber yang tak hanya secara teknis, tapi juga tata kelola. Serangan siber yang terus diterima Indonesia layaknya suatu tren yang terus meningkat, baik itu dari intensitas juga keragaman targetnya. Sektor vital seperti infrastruktur digital nasional, pemerintah daerah, dan layanan publik. Namun demikian, respon negara yang belum memadai, baik itu dari kemampuan deteksi dini, koordinasi antar penanggung jawab, sampai segi kecepatan penanganan kasus. Ketimpangan antara pusat dan daerah merupakan salah satu akar masalah pokok. Lemahnya koordinasi, kurangnya kapasitas daerah, dan dominasi teknologi asing sudah menjadikan Indonesia rentan terhadap serangan siber yang bersifat sistemik. Pendekatan yang bersifat sektoral dan tidak terintegrasi menjadikan strategi keamanan siber yang ada di Indonesia saat ini belum mampu membentuk sistem yang tangguh. Dalam konsep *resilience governance*, dapat dilihat dengan jelas bahwa Indonesia belum sepenuhnya mengadopsi prinsip yang ada seperti, fleksibilitas, adaptivitas, dan kontinuitas. Pendekatan pemerintah yang terlihat seperti sentralistik perlu diubah ke pendekatan yang lebih kolaboratif dan terstruktur. Terlebih lagi dengan proyeksi bahwa pemerintahan Prabowo mungkin akan lebih menekankan pendekatan militeristik dan efisiensi anggaran, maka penting



untuk menjaga keseimbangan antara aspek keamanan dan nilai-niali demokratis serta partisipatif.

Berdasarkan temuan yang ada, tulisan ini memberikan beberapa saran yang strategis. Kepada pemerintah pusat, khususnya Kementrian Komunikasi dan Informatika, Badan Siber dan Sandi Negara (BSSN), perlu dilakukan reformasi dalam kebijakannya seperti mendorong penguatan sistem deteksi dini namun tetap terintegrasi. Sistem ini diharapkan mampu memantau ancaman *real-time* dan memberi respon yang cepat tanpa adanya hambatan birokrasi. Untuk pemerintah daerah, sepertinya penting untuk meningkatkan kapasitas SDM dan kelembagaan melalui pelatihan keamanan siber yang berkelanjutan. Utamanya daerah di luar Jawa, perhatian khusus sangat diperlukan untuk membangun talenta digital yang mampu mendukung sistem keamanan digital pada tingkat lokal. Kepada sektor swasta, keterlibatan aktif dalam membentuk keamanan digital adalah kunci. Kolaborasi lewat lintas sektor dapat di adopsi demi mendapatkan solusi dan tindakan yang cepat. Terakhir, kepada pembuat kebijakan, penting rasanya untuk menciptakan sistem *check and balance* dalam proses perumusan kebijakan siber agar tak hanya dikuasai oleh pendekatan pertahanan dan keamanan saja. Indonesia memerlukan UU dan regulasi yang tak hanya reaktif terhadap serangan, akan tetapi juga preventif dan partisipatif dengan menjamin perlindungan hak warga negara. Jika Indonesia ingin membangun pertahanan digital yang sejati, maka arah kebijakan yang ada saat ini perlu bergeser, dari respon darurat menuju antisipasi yang cerdas; dari struktur yang tersentralisasi menuju tata kelola kolaboraitf; dari ketergantungan terhadap teknologi asing menuju inovasi lokal yang mampu bersaing.

6. DAFTAR PUSTAKA

Aji W., S. B. (2019). UPAYA MENINGKATKAN HASIL BELAJAR DAN KETERAMPILAN PROSES SISWA MELALUI MODEL PEMBELAJARAN PROBLEM BASED LEARNING DI KELAS IV SD N TINGKIR TENGAH 02. *Jurnal Basicedu, 3(1)*, 47-52.

Amindoni, A. (2021, May 21). *BBC*. Diambil kembali dari BPJS Kesehatan: Data ratusan juta peserta diduga bocor - 'Otomatis yang dirugikan masyarakat', kata pakar: https://www.bbc.com/indonesia/indonesia-57196905

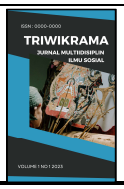
Anam, K. (2023, February 14). *Paling Rendah di ASEAN, Tingkat Literasi Digital RI Cuma 62%*. Diambil kembali dari CNBCIndonesia.com: https://www.cnbcindonesia.com/tech/20230214171553-37-413790/paling-rendah-di-asean-tingkat-literasi-digital-ri-cuma-62

Antara. (2021, November 24). *TNI AD Ingin Lebih Banyak Rekrut Ahli Siber Jadi Prajurit*. Diambil kembali dari Tempo.co: https://www.tempo.co/politik/tni-ad-ingin-lebih-banyak-rekrut-ahli-siber-jadi-prajurit--451032

Aptika, D. (2020, September 25). *Percepat Digitalisasi Layanan*. Diambil kembali dari kominfo.go.id: https://aptika.kominfo.go.id/2020/09/percepat-digitalisasi-layanan-pemerintah-konsolidasikan-pusat-data-nasional

Aswara, D. (2024, December 31). *Kaleidoskop 2024: 6 Serangan Siber Besar di Indonesia*. Diambil kembali dari Tempo.co: https://www.tempo.co/hukum/kaleidoskop-2024-6-serangan-siber-besar-di-indonesia-1188275

BBC. (2024, June 27). *Pusat Data Nasional Sementara lumpuh akibat ransomware, mengapa instansi pemerintah masih rentan terhadap serangan siber?* Diambil kembali dari BBC.com: https://www.bbc.com/indonesia/articles/cxee2985jrvo



Budin, A. R. (2024, August 24). *Krisis Tenaga Ahli Siber dan Dampaknya pada Keamanan Dunia*. Diambil kembali dari cyberhub.id: https://cyberhub.id/berita/dampak-krisis-tenaga-ahli-siber

Christianingrum, R., & Aida, A. N. (2021, January 20). *Analisis RUU Tentang APBN*. Diambil kembali dari Berkas.dpr.go: https://berkas.dpr.go.id/pa3kn/analisis-apbn/public-file/analisis-apbn-public-65.pdf

Diskominfo. (2024). *BSSN Sosialisasikan Standar dan Tata Cara Pelaksanaan Audit Keamanan SPBE Bagi Pemerintah Daerah*. Makassar: Diskominfo.

Edavos. (2024, August 20). *Kasus Cyber Crime Terbaru yang Mengguncang Indonesia Tahun 2024*. Diambil kembali dari edavos.com: https://edavos.com/kasus-cyber-crime/

Fauzi. (2023, February 6). *Menkomifo: Presiden Jokowi bangun infrastruktur digital daerah 3T*. Diambil kembali dari antaranew.com: https://www.antaranews.com/berita/3382719/menkomifo-presiden-jokowi-bangun-infrastruktur-digital-daerah-3t/

Feradhita. (2025, March 5). *Keamanan Siber di Indonesia: Ancaman & Tantangan yang Dihadapi*. Diambil kembali dari Logique.co.id: https://www.logique.co.id/blog/2025/03/05/keamanan-siber-di-indonesia

Fikrie, M. (2024, August 28). *Serangan Siber ke RI Naik 6 Kali Lipat pada H1 2024, Mayoritas dari Dalam Negeri*. Diambil kembali dari KumparanTech: https://kumparan.com/kumparantech/serangan-siber-ke-ri-naik-6-kali-lipat-pada-h1-2024-mayoritas-dari-dalam-negeri-23PnYQpafrf/full

Fitriana, S. N. (2024, January 7). *Prabowo-Gibran Mau Perkuat Pertahanan Siber Lewat Hilirisasi Digital*. Diambil kembali dari detikNews: https://news.detik.com/pemilu/d-7128734/prabowo-gibran-mau-perkuat-pertahanan-siber-lewat-hilirisasi-digital

Herman. (2022, October 24). *Marak Kebocoran Data, Indonesia Ternyata Kekurangan Tenaga Ahli Serangan Siber* . Diambil kembali dari Investor.id: https://investor.id/it-and-telecommunication/310738/marak-kebocoran-data-indonesia-ternyata-kekurangan-tenaga-ahli-serangan-siber

Ina. (2024, June 27). *Buruk Keamanan Siber di Indonesia Akibat Egosektoral*. Diambil kembali dari CNNIndonesia.com: https://www.cnnindonesia.com/nasional/20240627100303-20-1114729/buruk-keamanan-siber-di-indonesia-akibat-egosektoral

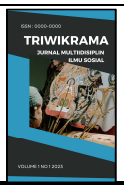
Kansong, U. (2024, June 25). Pusat Data Nasional Sementara lumpuh akibat ransomware, mengapa instansi pemerintah masih rentan terhadap serangan siber? (A. Akbar, Pewawancara)

Kusvianti, P., Ashari, A. P., & Izzah, A. N. (2023). Pandangan Ulrich Beck Tentang Risiko dan Ketidakpastian yang Dialami. *Jurnal Ilmiah Ecosystem*, 151.

Lavenia, A. (2024, July 3). *Berkat Brain Cipher, Kita Jadi Tahu Buruknya Keamanan Siber Indonesia*. Diambil kembali dari cxomedia.id: https://www.cxomedia.id/general-knowledge/20240703124844-55-180563/berkat-brain-cipher-kita-jadi-tahu-buruknya-keamanan-siber-indonesia

Lim, C. (2019, February 8). Indonesia Hanya Punya 21 Sensor Deteksi Dini Serangan Siber. (CNNIndonesia, Pewawancara) Diambil kembali dari CNNIndonesia.com: https://www.cnnindonesia.com/teknologi/20190208073502-192-367366/indonesia-hanya-punya-21-sensor-deteksi-dini-serangan-siber

Nestitie, D. P. (2025, April 12). *Kepercayaan Warga kepada Pemerintah, Modal Akselerasi Layanan Publik Berbasis Digital*. Diambil kembali dari Kompas.com: https://www.kompas.id/artikel/kepercayaan-warga-kepada-pemerintah-modal-akselerasi-layanan-publik-berbasis-digital



Prabowo, T. B., & Sihaloho, R. A. (2023). ANALISIS KETERGANTUNGAN INDONESIA PADA TEKNOLOGI ASING DALAM. *Lemhannas RI*, 73.

Putra, A. M. (2024, May 14). *"Masyarakat Risiko" dan Demokrasi*. Diambil kembali dari Kompas.id: https://www.kompas.id/baca/opini/2024/05/13/masyarakat-risiko-dan-demokrasi

Putra, K. I. (2019, January 16). Belajar Dari Tata Kelola Keamanan Siber Singapura. *Center for Digital Society*, 2. Diambil kembali dari cfds.fisipol.ugm: https://cfds.fisipol.ugm.ac.id/wp-content/uploads/sites/1423/2021/01/44-CfDS-Case-Study-Belajar-dari-Tata-Kelola-Keamanan-Siber-Singapura.pdf

R, A. (2025, April 9). *Kebocoran Data Pemalang: Situs Resmi Pemerintah Diretas, Ini Tanggapan dan Analisis Pakar*. Diambil kembali dari fourtrezz.co.id: https://fourtrezz.co.id/kebocoran-data-pemalang-situs-resmi-pemerintah-diretas-ini-tanggapan-dan-analisis-pakar/

Rachmania, M. (2021, July 28). *Diskusi Bulanan DIHI UGM: Negotiating Resilience in Jakarta's Climate Change Governance*. Diambil kembali dari hi.fisipol.ugm.ac.id: https://hi.fisipol.ugm.ac.id/diskusi-bulanan-dihi-ugm-negotiating-resilience-in-jakartas-climate-change-governance

Ramadhan, F. (2024, November 20). *Indonesia Kekurangan Tenaga Ahli Keamanan Siber*. Diambil kembali dari MediaIndonesia.com: https://mediaindonesia.com/teknologi/719605/indonesia-kekurangan-tenaga-ahli-keamanan-siber

Safitri, K. (2024, October 14). *10 Tahun Pemerintahan Jokowi, Upaya Pemberantasan Kejahatan Siber Terus Meningkat*. Diambil kembali dari nasional.kompas.com: https://nasional.kompas.com/read/2024/10/14/11503981/10-tahun-pemerintahan-jokowi-upaya-pemberantasan-kejahatan-siber-terus?page=all

Sari, F. K. (2024, August 26). *Peran Artificial Intelligence dalam Keamanan Siber*. Diambil kembali dari csirt.teknorat.ac.id: https://csirt.teknokrat.ac.id/peran-artificial-intelligence-dalam-keamanan-siber/

Singgih, Y. (2025, January 23). *Menelusuri Jejak Insiden Kebocoran Data Kesehatan*. Diambil kembali dari Cyberhub.id: https://cyberhub.id/berita/jejak-insiden-kebocoran-data-kesehatan

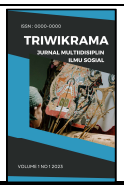
Teknokrat. (2025, November 21). *Opini: Pentingnya Keamanan Informasi dalam Dunia Digital*. Diambil kembali dari ftik.teknokrat: https://ftik.teknokrat.ac.id/opini-pentingnya-keamanan-informasi-dalam-dunia-digital/

Wahidin, K. P. (2024, November 11). *Di balik keroposnya pertahanan siber Indonesia*. Diambil kembali dari alinea.id: https://www.alinea.id/peristiwa/di-balik-keroposnya-pertahanan-siber-indonesia

Wijaya, A. (2024, June 29). *Habis Bjorka, Terbitlah Lockbit: Kominfo dan BSSN Keok!* Diambil kembali dari monitorindonesia.com: https://monitorindonesia.com/investigasi/read/2024/06/590539/habis-bjorka-terbitlah-lockbit-kominfo-dan-bssn-keok

Yanuar, Y. (2024, June 27). *Serangan Siber pada Pusat Data Nasional Menarik Perhatian Media Internasional*. Diambil kembali dari Tempo.co: https://www.tempo.co/ekonomi/serangan-siber-pada-pusat-data-nasional-menarik-perhatian-media-internasional-45466

Yaputra, H. (2024, September 21). *Daftar Kebocoran Data Pribadi di Era Jokowi, Paling Banyak di Instansi Pemerintah*. Diambil kembali dari Tempo.co:



https://www.tempo.co/politik/daftar-kebocoran-data-pribadi-di-era-jokowi-paling-banyak-di-instansi-pemerintah--7403

Zamzama, A. (2024, November 1). *Melihat Kasus Karangan Bunga BEM Unair, Ini Angka Bulanan Serangan Siber di Indonesia*. Diambil kembali dari GoodStats: https://goodstats.id/article/buntut-kasus-karangan-bunga-bem-unair-serangan-siber-kembali-terjadi-ll9Lx

Zulfikar, R. A. (2024, June 25). *Lemahnya Keamanan Siber pada Instansi Pemerintah*. Diambil kembali dari Depokpos.com: https://www.depokpos.com/2024/06/lemahnya-keamanan-siber-pada-instansi-pemerintah/