Kreatif: Jurnal Pengabdian Masyarakat Nusantara
Volume 6, Nomor 1, Maret 2026
e-ISSN: 2962-3839; p-ISSN: 2962-4436, Hal. 570-586
DOI: https://doi.org/10.55606/kreatif.v6i1.10750
Tersedia: https://researchhub.id/index.php/kreatif

Dilema Transparansi dan Fragmentasi dalam Pendanaan Pertahanan Siber Indonesia

The Dilemma of Transparency and Fragmentation in Indonesia's Cyber Defense Funding

Rachel Juliana Wulan Sumampouw[1*], Aris Sarjito[2], Herlina Tarigan[3]
[1-3]Manajemen Pertahanan, Fakultas Manajemen Pertahanan, Universitas Pertahanan Republik Indonesia
**Penulis Korespondensi: racheljwsumampouw@gmail.com*

Riwayat artikel:
Naskah Masuk: 21 Desember 2025;
Revisi: 19 Januari 2026;
Diterima: 01 Februari 2026;
Tersedia: 04 Februari 2026;

Keywords*: Cyber Defense; Fiscal Transparency; Institutional Fragmentation; Securitization; State Budget.*

Abstract*. This article examines the disparity between escalating cyber threats and cyber defense financing in Indonesia over the 2015–2025 period. Using a non-systematic qualitative literature review and an analysis of open budget data (2017–2023), the study highlights a dispersed and volatile pattern of cybersecurity spending allocations, amounting to only around 0.02% of GDP. The analytical framework draws on the concepts of securitization, fiscal governance, and institutional architecture. The findings reveal a structural gap between political rhetoric and actual funding, weak fiscal transparency in the security sector, and fragmentation across key institutions such as BSSN, the Ministry of Communication and Informatics, and the Ministry of Defense. These results indicate that without a reorientation of budget priorities, cross-sector policy integration, and tiered improvements in transparency, Indonesia risks persistent systemic vulnerabilities in national digital security. The study recommends establishing a "Cyber Defense and Resilience" program within the state budget (APBN) as an initial step toward more strategic and coordinated financing reform.*

Abstrak

Artikel ini mengkaji ketimpangan antara eskalasi ancaman siber dan pembiayaan pertahanan siber di Indonesia dalam periode 2015–2025. Melalui tinjauan literatur kualitatif non-sistematis dan analisis data anggaran terbuka (2017–2023), studi ini menyoroti dinamika alokasi belanja keamanan siber yang tersebar dan fluktuatif, dengan proporsi hanya sekitar 0,02% dari PDB. Kerangka analisis berlandaskan pada konsep sekuritisasi, tata kelola fiskal, dan arsitektur kelembagaan. Hasil kajian menunjukkan adanya kesenjangan struktural antara retorika politik dan pendanaan aktual, lemahnya transparansi fiskal di sektor keamanan, serta fragmentasi antar lembaga seperti BSSN, Kominfo, dan Kementerian Pertahanan. Temuan ini menegaskan bahwa tanpa penataan ulang prioritas anggaran, integrasi kebijakan lintas sektor, dan peningkatan transparansi berjenjang, Indonesia berisiko menghadapi kerentanan sistemik dalam keamanan digital nasional. Studi ini merekomendasikan pembentukan program "Pertahanan Siber dan Ketahanan" dalam APBN sebagai langkah awal reformasi pembiayaan yang lebih strategis dan terkoordinasi.

Kata kunci: Anggaran Negara; Fragmentasi Institusional; Pertahanan Siber; Sekuritisasi; Transparansi Fiskal.

1. LATAR BELAKANG

Lanskap keamanan Indonesia tengah mengalami perubahan signifikan seiring percepatan digitalisasi. Meski menjadi salah satu negara dengan pertumbuhan ekonomi digital tercepat di ASEAN, Indonesia juga mencatat jumlah lalu lintas siber berbahaya dan insiden kebocoran data tertinggi di kawasan, seperti kasus Bjorka, kebocoran data KPU, dan serangan terhadap fasilitas kesehatan (Purwandari, 2024). Dinamika ini mendorong isu keamanan siber dan "kedaulatan siber" semakin menonjol dalam pidato presiden, strategi nasional, hingga dokumen putih pertahanan. Namun, sejumlah studi terbaru menunjukkan bahwa proses

sekuritisasi tersebut masih banyak bersifat retorik: ancaman siber kerap digambarkan sebagai ancaman eksistensial, tetapi respons dalam bentuk alokasi anggaran dan penguatan institusi belum sejalan (Primawanti et al., 2024).

Di sisi lain, anggaran pertahanan Indonesia terus meningkat secara absolut, meskipun pemerintah masih menghadapi tekanan fiskal dan berbagai prioritas sosial yang mendesak. Beragam studi mengenai hubungan antara belanja pertahanan dan pertumbuhan ekonomi di Indonesia maupun negara berkembang menunjukkan bahwa dampaknya bisa positif, negatif, atau netral. Tergantung pada struktur belanja, kualitas institusi, serta biaya peluangnya (Dudzevičiūtė et al., 2021). Namun, hanya sebagian kecil dari anggaran tersebut yang tampaknya diarahkan pada pembangunan kapasitas siber, yang sebagian besar justru berada di luar lingkup Kementerian Pertahanan, seperti BSSN, Kominfo, dan regulator infrastruktur kritis. Purwandari (2024) memperkirakan bahwa Indonesia hanya mengalokasikan sekitar 0,02% dari PDB untuk keamanan siber, angka yang jauh tertinggal dibandingkan negara-negara ASEAN lainnya.

Dilihat melalui lensa teori sekuritisasi, ketika elit politik dan dokumen resmi negara telah membingkai ancaman siber sebagai ancaman eksistensial terhadap keberlangsungan negara, seharusnya terdapat implikasi normatif yang jelas terhadap tata kelola anggaran dan kelembagaan. Logika sekuritisasi menegaskan bahwa isu yang diposisikan sebagai ancaman eksistensial idealnya diikuti oleh "tindakan luar biasa", yang mencakup penetapan prioritas pendanaan, pembentukan instrumen kelembagaan khusus, serta pengembangan mekanisme pelaporan publik yang lebih strategis dan terintegrasi (Buzan et al., 1998; Otukoya & Otukoya, 2024). Dalam konteks pertahanan siber, hal ini berarti bahwa narasi tentang "kedaulatan siber" dan "ancaman eksistensial" seharusnya diterjemahkan ke dalam alokasi anggaran yang lebih stabil dan meningkat, program jangka panjang lintas kementerian/lembaga, serta indikator kinerja yang eksplisit.

Secara normatif, batas "kewajaran" belanja keamanan siber juga dapat dirumuskan dengan merujuk pada pengalaman internasional. Analisis kebijakan Uni Eropa serta laporan *European Court of Auditors* menunjukkan bahwa secara global, total belanja keamanan siber baik publik maupun privat diperkirakan berada di kisaran 0,1% dari PDB. Di Amerika Serikat, angka tersebut bahkan mencapai sekitar 0,35% dari PDB, dengan belanja pemerintah federal saja berada pada kisaran 0,1% dari PDB (European Court of Auditors, 2019). Bagi negara yang tergolong *emerging digital economy* seperti Indonesia, proporsi sekitar 0,1% dari PDB dapat dipandang sebagai lower bound normatif bagi investasi pertahanan siber yang dapat dianggap kredibel.

Dari perspektif tata kelola, rekomendasi OECD mengenai open government dan transparansi anggaran menegaskan bahwa seluruh program sektor publik (termasuk sektor pertahanan) pada prinsipnya harus memenuhi standar minimum keterbukaan, yakni penyediaan informasi fiskal yang relevan secara lengkap, tepat waktu, sistematis, dan mudah diakses oleh publik (OECD, 2017, 2019). Dalam praktiknya, Indonesia telah menunjukkan kemajuan penting dalam digitalisasi anggaran, peningkatan transparansi fiskal, serta penerapan prinsip pemerintahan terbuka melalui reformasi e-budgeting dan berbagai inisiatif data terbuka yang memperluas akses publik terhadap informasi anggaran (Oktaviani et al., 2019; Salahudin et al., 2024). namun, kemajuan tersebut belum terdistribusi secara merata di seluruh sektor. Pengeluaran pertahanan dan keamanan, termasuk keamanan siber, masih menjadi salah satu area yang paling minim transparansi, sejalan dengan tren global tetapi juga mencerminkan warisan historis Indonesia berupa pembiayaan militer di luar anggaran resmi serta lemahnya mekanisme pengawasan sipil (Hafel & Hi Ibrahim, 2024). Kajian terbaru tentang politik anggaran menunjukkan bahwa fragmentasi proses penganggaran, keterbatasan pengawasan parlemen, dan ketidakjelasan teknis terus menghambat kemampuan negara untuk mengalokasikan sumber daya secara strategis di sektor keamanan. Dengan demikian, ketertinggalan Indonesia baik dalam hal besaran alokasi anggaran maupun tingkat keterbukaan informasi tidak hanya merupakan persoalan empiris, tetapi juga mencerminkan jarak yang signifikan dari standar normatif tata kelola pertahanan siber yang ideal.

Secara keseluruhan, berbagai dinamika tersebut mengarah pada satu persoalan inti: meskipun Indonesia semakin menekankan urgensi keamanan siber dan terus meningkatkan belanja pertahanan secara umum, kapasitas pertahanan siber dan tata kelola keuangan negara belum tentu berkembang seiring dengan retorika tersebut. Penelitian ini berupaya menjawab pertanyaan utama: *Bagaimana prioritas anggaran, pengaturan transparansi, dan praktik kelembagaan Indonesia membentuk kemampuannya untuk membiayai pertahanan siber yang efektif?*

Dalam artikel ini, istilah *keamanan siber* digunakan sebagai payung yang merujuk pada upaya perlindungan ekosistem digital secara luas (pemerintah, sektor privat, dan masyarakat), sedangkan *pertahanan siber* dipakai untuk menekankan dimensi negara, terutama perlindungan aset strategis, infrastruktur kritis, serta jaringan pertahanan/militer dan C4ISR. Karena fokus penelitian ini adalah pembiayaan pada dimensi negara, istilah utama yang digunakan adalah *pembiayaan pertahanan siber*. Namun, ketika merujuk pada indikator komparatif yang dalam literatur disebut sebagai *cybersecurity spending* (misalnya estimasi

belanja sebagai persentase PDB), artikel ini tetap menggunakan istilah *keamanan siber* agar konsisten dengan sumber data.

Artikel ini memberikan tiga kontribusi utama. Pertama, artikel ini menyajikan sintesis terarah dari literatur Indonesia dan internasional yang berkembang mengenai pembiayaan pertahanan siber. Kedua, artikel ini menggabungkan data insiden keamanan siber dengan informasi anggaran untuk menyoroti ketidakseimbangan antara alokasi pembiayaan dan kapasitas yang tersedia. Ketiga, artikel ini menawarkan kerangka konseptual yang dapat digunakan untuk menyelaraskan pembiayaan pertahanan siber dengan agenda reformasi manajemen pertahanan dan tata kelola keuangan publik yang lebih luas di Indonesia.

2. KAJIAN TEORITIS

Pertahanan Siber, Sekuritisasi, dan Kapasitas Negara

Secara umum, pertahanan siber dipahami sebagai serangkaian kebijakan, institusi, dan langkah teknis yang dirancang oleh negara untuk melindungi aset digital, infrastruktur kritis, serta jaringan militer dari berbagai bentuk agresi siber (Saeed et al., 2023). Di Indonesia, fungsi pertahanan siber tersebar di berbagai lembaga, termasuk Kementerian Pertahanan, satuan siber TNI, BSSN, Kementerian Kominfo, serta regulator sektoral seperti OJK untuk sektor keuangan. Fatihah (2021) mencatat bahwa meskipun Indonesia telah menyusun strategi keamanan siber nasional dan menetapkan sejumlah regulasi pendukung, pelaksanaannya masih bersifat terfragmentasi dan belum konsisten di seluruh sektor.

Fragmentasi kelembagaan ini tidak hanya menimbulkan persoalan koordinasi, tetapi juga mempunyai konsekuensi fiskal: anggaran pertahanan siber diajukan dan dikelola secara terpisah oleh masing-masing aktor, sehingga rentan terhadap duplikasi program, kesenjangan pendanaan di area tertentu, dan ketiadaan kerangka pembiayaan jangka panjang yang terintegrasi (Alfath & Cahya, 2024; Purwandari, 2024)

Berdasarkan kerangka teori sekuritisasi, Primawanti et al., (2024) menunjukkan bahwa para elit di Indonesia semakin memposisikan ancaman siber sebagai isu yang menyangkut kelangsungan hidup negara. Namun, “tindakan luar biasa” yang seharusnya mengikuti proses sekuritisasi, yaitu mulai dari pembentukan institusi yang lebih terpadu, pendanaan yang berkelanjutan, hingga mandat yang jelas, belum sepenuhnya terwujud. Kesenjangan antara retorika dan realitas pendanaan inilah yang menjadi kunci untuk memahami dinamika pembiayaan pertahanan siber di Indonesia.

Literatur mengenai kapasitas keamanan siber menegaskan bahwa investasi di bidang ini bukan semata persoalan teknis, melainkan juga mencerminkan kapasitas negara dan kualitas

tata kelola. Dutton et al., (2019) menemukan bahwa negara-negara dengan tingkat "kapasitas keamanan siber" yang lebih tinggi (diukur melalui aspek hukum, teknis, organisasional, dan sumber daya manusia) cenderung memperoleh hasil sosial-ekonomi yang lebih baik. Sementara itu, penelitian oleh Saeed et al., (2023) menunjukkan bahwa percepatan transformasi digital meningkatkan paparan terhadap risiko siber, sehingga ketahanan yang efektif membutuhkan investasi berkelanjutan yang didasarkan pada penilaian risiko, bukan sekadar pengeluaran ad hoc sebagai respons terhadap insiden besar.

Pengeluaran Pertahanan, Keamanan, dan Pengembangan

Hubungan antara pengeluaran pertahanan dan perkembangan ekonomi telah lama menjadi perdebatan dalam literatur. Berbagai analisis meta dan studi lintas negara menunjukkan temuan yang beragam, bergantung pada periode analisis, tingkat pendapatan negara, serta model empiris yang digunakan (Solanki et al., 2023). Pada konteks negara-negara Baltik, Dudzevičiūtė (2021) menemukan bahwa pengeluaran pertahanan dapat mendorong pembangunan berkelanjutan apabila terintegrasi dengan kerangka keamanan dan tata kelola yang komprehensif. Sementara itu, penelitian mengenai negara-negara berkembang mengindikasikan bahwa belanja militer dapat memberikan kontribusi positif terhadap pertumbuhan ekonomi ketika diarahkan pada kapasitas produktif, seperti penguatan industri dalam negeri atau riset dan pengembangan *(R&D*) dengan kegunaan ganda, tetapi dapat menghambat pertumbuhan ketika didominasi oleh biaya personel dan peralatan impor (Acosta et al., 2018; Bogdanoski & Nikolov, 2007; Lu et al., 2016; Nozadze, 2018).

Namun, sebagian besar studi tersebut memperlakukan belanja pertahanan sebagai variabel agregat tunggal tanpa memisahkan komponen-komponen baru seperti pertahanan siber, intelijen, dan C4ISR. Dalam kasus Indonesia, misalnya, studi Putra et al. (2019) hanya menggunakan data pengeluaran militer total tanpa disaggregasi fungsi, sehingga dinamika alokasi ke program siber tidak tertangkap di dalam model. Dengan kata lain, pertahanan siber cenderung menjadi "komponen tak terlihat" dalam literatur belanja pertahanan dan pembangunan: sekalipun belanja pertahanan meningkat, tidak ada jaminan bahwa porsi anggaran untuk kapabilitas siber ikut naik secara proporsional. Kondisi ini menjadi relevan dalam pembahasan Indonesia karena indikator pendanaan siber yang tersedia justru menunjukkan volatilitas anggaran lembaga siber dan rendahnya belanja siber relatif terhadap PDB.

Kajian yang berfokus pada Indonesia juga menunjukkan hasil yang beragam. Saputro et al., (2021) dan Soelistyo (2023) menemukan adanya hubungan positif jangka panjang antara pengeluaran pertahanan dan pertumbuhan PDB, sementara Putra et al., (2019) melaporkan

tidak terdapat kausalitas yang signifikan. Namun, terlepas dari perbedaan hasil tersebut, sebagian besar studi ini cenderung memperlakukan "pertahanan" sebagai kategori tunggal tanpa memisahkannya ke dalam komponen seperti siber, intelijen, atau kekuatan konvensional. Akibatnya, pengeluaran yang berkaitan dengan kemampuan siber tidak terlihat secara konseptual dalam model-model agregat tersebut, yang pada akhirnya turut menjelaskan mengapa sektor ini sering kurang diprioritaskan.

Transparansi Keuangan Publik, *E-Budgeting*, dan Sektor Keamanan

Transparansi fiskal dan digitalisasi anggaran memegang peran penting dalam memastikan bahwa pengeluaran keamanan dijalankan secara efisien dan memiliki legitimasi publik. Dewi dan Prasojo (2021) menemukan bahwa keterbukaan anggaran serta penyampaian informasi fiskal secara proaktif dapat meningkatkan kepercayaan masyarakat secara signifikan, terutama ketika data disajikan dalam format yang mudah diakses dan dipahami. Reformasi *e-budgeting*, termasuk platform online dan sistem keuangan yang *interoperable*, telah dipromosikan untuk mengurangi risiko korupsi dan meningkatkan akuntabilitas (Oktaviani et al., 2019; Salahudin et al., 2024).

Di tingkat global, standar *open budgeting* menekankan bahwa proses anggaran yang baik harus menyediakan informasi yang komprehensif, tepat waktu, dan dapat dibandingkan bagi publik di seluruh siklus anggaran. OECD, melalui *Recommendation on Open Government dan Budget Transparency Toolkit*, mendorong agar seluruh program sektor publik termasuk pertahanan memenuhi standar minimum keterbukaan atas tujuan, alokasi, dan hasil kebijakan fiskal publik (OECD, 2017, 2019).

Oktaviani (2019) menemukan bahwa penerapan e-budgeting dapat memperkuat transparansi dan akuntabilitas di tingkat pemerintah daerah di Indonesia. Namun, mereka menekankan bahwa efektivitas sistem tersebut sangat bergantung pada komitmen politik serta kualitas data yang tersedia. Sementara itu, Salahudin (2024) melalui analisis bibliometrik, menunjukkan bahwa kajian mengenai anggaran digital semakin beralih ke isu partisipasi publik, mekanisme pengawasan, dan integrasinya dengan agenda reformasi tata kelola digital yang lebih luas.

Meski demikian, penganggaran di sektor keamanan dan pertahanan kerap dikecualikan dari tingkat transparansi penuh dengan alasan kerahasiaan dan perlindungan keamanan nasional. Literatur mengenai "pemerintahan di era digital" menekankan bahwa pengecualian semacam ini harus diterapkan secara sangat terbatas dan tetap diseimbangkan dengan tuntutan akuntabilitas publik, terutama dalam bidang berisiko tinggi seperti kegiatan pengawasan dan operasi siber. Dalam konteks Indonesia, Laksmana (2014) serta analisis-analisis berikutnya

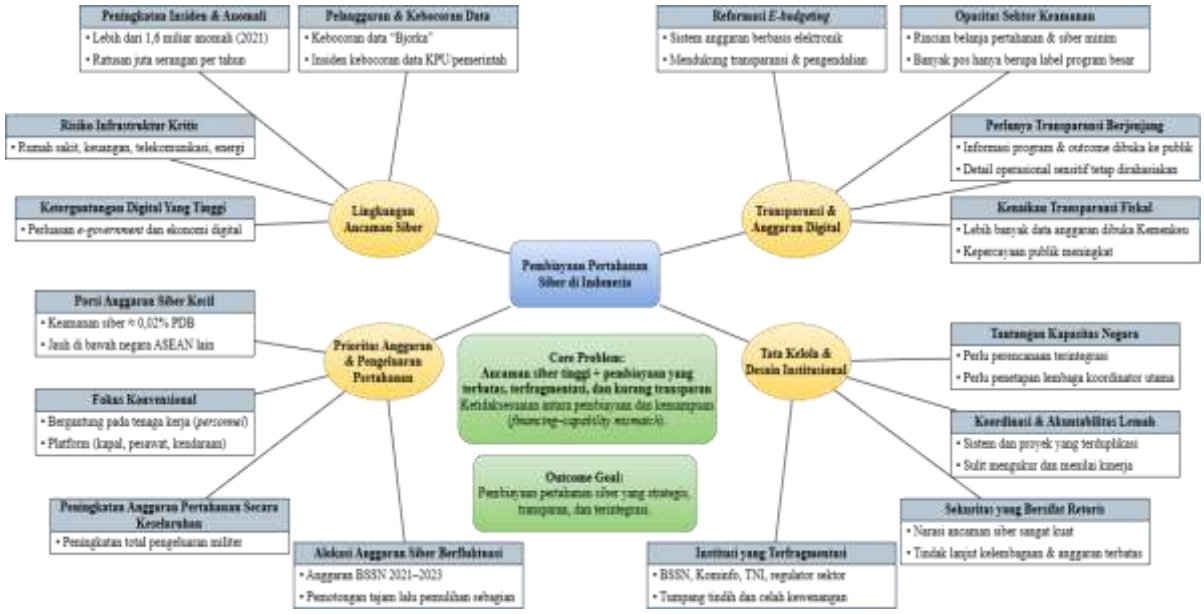
menunjukkan bahwa praktik historis aktivitas militer di luar anggaran (yang bersifat tidak transparan) telah melemahkan disiplin fiskal dan kontrol sipil. Reformasi yang dilakukan sejauh ini pun baru mampu menangani sebagian kecil dari persoalan tersebut (Hafel & Hi Ibrahim, 2024; Khaw et al., 2024).

Investasi & Tata Kelola Keamanan Siber di Indonesia

Sejumlah studi terbaru yang menyoroti konteks Indonesia menawarkan gambaran yang lebih mendalam mengenai pola pembiayaan siber nasional. Purwandari (2024) memperkirakan bahwa belanja Indonesia untuk keamanan siber hanya mencapai sekitar 0,02% dari PDB, jauh lebih rendah dibandingkan negara sekelasnya, seperti Singapura (~0,22%) dan Malaysia (~0,10%). Kesenjangan ini mengindikasikan bahwa kapasitas pertahanan siber Indonesia berpotensi tertinggal dalam kompetisi ketahanan digital regional, terutama pada investasi teknologi, penguatan SDM, dan perlindungan infrastruktur kritis. Sementara itu, data BSSN mencatat lebih dari 1,6 miliar anomali siber pada 2021 serta 347 juta insiden hanya dalam enam bulan pertama tahun 2023. Di sisi regulasi, Alfath & Cahya (2024) menemukan bahwa meskipun terjadi perkembangan normatif yang cukup signifikan dalam periode 2020–2023, kerangka keamanan siber Indonesia masih menghadapi sejumlah persoalan, termasuk tumpang tindih mandat, penegakan hukum yang tidak konsisten, dan koordinasi antarlembaga yang lemah.

Penelitian dalam bidang ilmu politik mengenai hukum dan ekonomi digital di Indonesia menunjukkan bahwa kejahatan siber, penipuan daring, dan kebocoran data telah berkembang menjadi permasalahan yang meluas. Temuan-temuan tersebut juga menegaskan bahwa tata kelola yang efektif (meliputi regulasi yang jelas, penegakan hukum yang kuat, serta transparansi) sangat diperlukan untuk melindungi masyarakat dan menjaga stabilitas pasar (Marwan & Bonfigli, 2022; Meidyasari, 2024). Namun demikian, literatur juga mencatat bahwa tanggung jawab regulasi masih tersebar di berbagai institusi, masing-masing dengan siklus anggaran dan mekanisme akuntabilitas yang berbeda, sehingga menyulitkan koordinasi dan konsistensi kebijakan. Dari sisi pembiayaan, konfigurasi multi-aktor ini cenderung mendorong penganggaran yang terfragmentasi (silo), meningkatkan risiko duplikasi program, dan menyulitkan evaluasi biaya–manfaat serta capaian kinerja lintas lembaga.

Peta Konseptual



Keterangan: Disusun penulis berdasarkan sintesis literatur dan data sekunder.

Gambar 1. Peta Konsep pembiayaan pertahanan siber di Indonesia.

Keterkaitan antara ancaman siber, prioritas anggaran, transparansi, dan tata kelola digambarkan dalam peta konseptual (Gambar 1). Inti dari peta ini adalah pembiayaan pertahanan siber di Indonesia, yang dikelompokkan ke dalam empat kluster utama: lanskap ancaman siber, prioritas anggaran dan pola belanja pertahanan, transparansi serta digitalisasi anggaran, dan akhirnya, tata kelola serta desain institusional.

3. METODE PENELITIAN

Penelitian ini menerapkan pendekatan deskriptif kualitatif melalui tinjauan literatur non-sistematis, yang dilengkapi dengan data kuantitatif sekunder berupa angka anggaran dan visualisasi deskriptif sederhana. Pendekatan deskriptif kualitatif dipilih untuk menyajikan gambaran yang sistematis, faktual, dan kritis tentang bagaimana pembiayaan pertahanan siber di Indonesia dijalankan, tanpa bergantung pada pengujian hipotesis statistik (Lambert & Lambert, 2012; Sandelowski, 2000). Fokus utama penelitian ini adalah memahami keterkaitan antara ancaman siber, prioritas anggaran, praktik transparansi, dan pengaturan institusional yang membentuk pembiayaan pertahanan siber di Indonesia. Sejalan dengan karakter tinjauan non-sistematis, tujuan penelitian adalah menyintesis dan menafsirkan secara kritis pengetahuan yang tersedia, bukan memetakan bukti secara exhaustif seperti SLR (Snyder, 2019).

Analisis dalam penelitian ini bertumpu pada data sekunder yang diperoleh dari publikasi akademik dan dokumen resmi. Korpus utama mencakup artikel jurnal terindeks dan makalah

konferensi yang telah melalui proses peer review, terutama yang diterbitkan dalam satu dekade terakhir. Sumber-sumber tersebut dilengkapi dengan dokumen kebijakan nasional yang relevan, laporan anggaran, serta berbagai asesmen terkait keamanan siber di Indonesia (Snyder, 2019). Pemilihan sumber dilakukan melalui penelusuran bertahap, dengan kata kunci yang menggabungkan "Indonesia", "*cybersecurity/cyber defense*", "*budget/defence expenditure*", "*transparency*", "*e-budgeting*", dan "*governance*", kemudian dilanjutkan dengan *citation tracking* untuk menemukan rujukan kunci yang sering dikutip. Sumber dimasukkan apabila relevan langsung dengan fokus pembiayaan/tata kelola pertahanan siber, memiliki kualitas akademik yang dapat ditelusuri, dan menyediakan informasi konseptual/empiris yang memadai; sementara sumber non-akademik seperti blog/opini tidak digunakan sebagai rujukan utama. Untuk meminimalkan *selection bias*, literatur diambil dari beberapa klaster tema (ancaman, anggaran, transparansi, tata kelola) dan mencakup temuan yang beragam (konvergen maupun berbeda). Hal ini menunjukkan penggunaan tinjauan literatur naratif dan non-sistematis untuk mensintesis dan menafsirkan secara kritis pengetahuan yang ada, daripada memetakan secara menyeluruh.

Studi ini juga mencakup data deskriptif sederhana. Informasi anggaran untuk Badan Siber dan Sandi Negara (BSSN) periode data anggaran 2021–2023 diperoleh dari dokumen anggaran negara yang tersedia secara publik dan analisis parlemen yang diterbitkan oleh Kementerian Keuangan dan Komisi Anggaran Dewan Perwakilan Rakyat (Kementerian Keuangan RI, 2022; DPR RI, 2023). Data anggaran diproses dengan menyelaraskan satuan pelaporan, memastikan konsistensi tahun anggaran, serta merangkum angka ke dalam tabel dan grafik untuk menonjolkan tren perubahan antar tahun; angka kemudian dicek silang terhadap lebih dari satu dokumen resmi ketika tersedia untuk meningkatkan keterandalan. Angka perbandingan pengeluaran keamanan siber sebagai persentase dari PDB di negara-negara ASEAN terpilih diambil dari penelitian empiris terbaru tentang investasi keamanan siber Indonesia (Purwandari, 2024). Angka-angka ini disajikan melalui grafik dasar untuk menggambarkan tren dan posisi relatif, melengkapi interpretasi kualitatif daripada berfungsi sebagai dasar untuk pengujian statistik formal.

Sintesis dilakukan melalui pemetaan tematik yang menghubungkan temuan literatur dan data anggaran ke dalam empat klaster analitis: (1) lingkungan ancaman siber, (2) prioritas anggaran dan komposisi belanja pertahanan, (3) transparansi dan *digital budgeting*, serta (4) tata kelola dan desain kelembagaan. Pemetaan ini menjadi dasar penyusunan peta konseptual dan digunakan untuk menafsirkan bagaimana pola pendanaan yang tampak dalam data

anggaran berkaitan dengan narasi ancaman, prioritas fiskal, tingkat keterbukaan, dan fragmentasi kelembagaan.

4. HASIL DAN PEMBAHASAN

Hasil Temuan

Eskalasi Ancaman dan Indikator Kapasitas

Literatur dan data pemantauan menunjukkan eskalasi ancaman siber yang signifikan dalam beberapa tahun terakhir. Lebih dari 1,6 miliar anomali lalu lintas siber tercatat pada 2021, dan ratusan juta insiden spesifik seperti malware, phishing, dan intrusi terjadi hanya dalam enam bulan pertama tahun 2023 (Purwandari, 2024). Insiden yang menargetkan lembaga pemerintah, BUMN, serta infrastruktur kritis (misalnya rumah sakit dan jaringan telekomunikasi) mengindikasikan bahwa aktivitas siber agresif telah menembus sektor strategis negara dan ekonomi. Dalam dimensi kapasitas, posisi Indonesia dalam Indeks Keamanan Siber Global ITU memang menunjukkan perbaikan, tetapi masih tertinggal dibandingkan pemimpin regional seperti Singapura dan Malaysia, terutama pada aspek teknis dan pembangunan kapasitas (Fatihah, 2021).

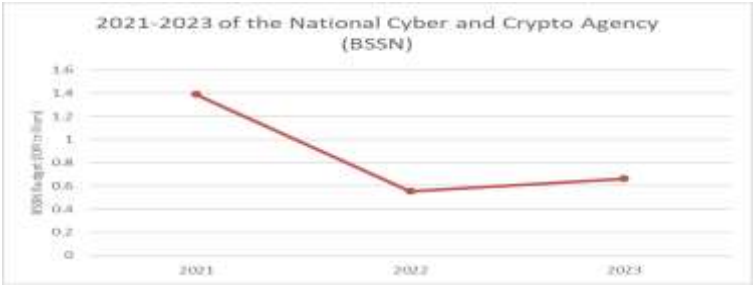
Fluktuasi Anggaran BSSN (2021-2023)

Dari sisi pembiayaan, data anggaran menunjukkan bahwa alokasi untuk sektor siber masih relatif kecil dan berfluktuasi. Anggaran BSSN tercatat sekitar IDR 1,39 triliun pada 2021, turun drastis menjadi sekitar IDR 554,6 miliar pada 2022, kemudian meningkat kembali secara parsial menjadi sekitar IDR 662,4 miliar pada 2023 (lihat Tabel 1 dan Gambar 2).

Tabel 1. Anggaran BSSN 2021-2023.

Tahun	Anggaran BSSN (IDR Triliun)
2021	1,39
2022	0,5546
2023	0,6624

Sumber: Kementerian Keuangan RI (2022) dan DPR RI (2023).



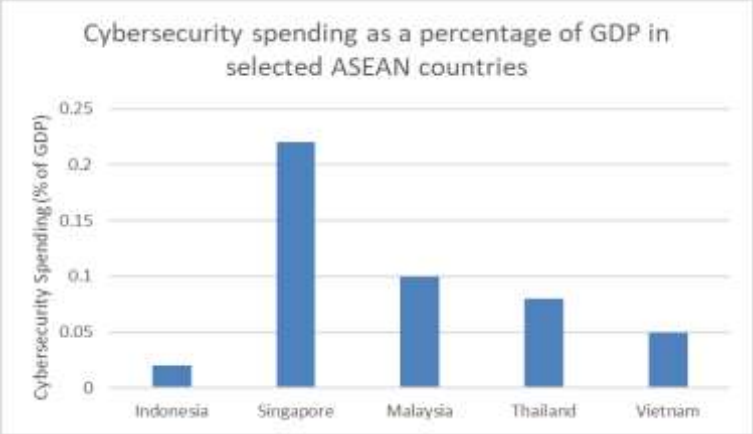
Gambar 2. Tren anggaran BSSN 2021-2023 (IDR Triliun).

Sumber: Kementerian Keuangan RI (2022) dan DPR RI (2023), diolah penulis.

Keterangan: diolah dari dokumen APBN yang dipublikasikan Kementerian Keuangan RI dan ringkasan/pembahasan RAPBN di DPR RI.

Perbandingan Belanja Keamanan Siber Sebagai Persentase PDB (ASEAN terpilih)

Perbandingan regional memperlihatkan posisi investasi Indonesia yang relatif rendah. Belanja Indonesia untuk keamanan siber diperkirakan sekitar 0,02% dari PDB, lebih rendah dibandingkan Singapura (~0,22%) dan Malaysia (~0,10%), serta masih di bawah Thailand (~0,08%) dan Vietnam (~0,05%) (Purwandari, 2024) (lihat Gambar 3).



Gambar 3. Belanja Keamanan Siber sebagai % PDB (ASEAN).

Sumber: Purwandari (2024).

Keterangan: Angka merupakan estimasi belanja keamanan siber (% PDB)

Pembahasan

Financing-capability Mismatch: Gap antara Eskalasi Ancaman dan Realisasi Fiskal

Temuan di atas mengindikasikan adanya *financing–capability mismatch* pada pertahanan siber Indonesia: eskalasi ancaman tidak diikuti pola pendanaan yang stabil dan berorientasi kapasitas. Penurunan anggaran BSSN pada 2022, ketika tekanan ancaman membesar, mencerminkan bahwa program pertahanan siber cenderung diperlakukan sebagai pos yang mudah disesuaikan secara fiskal, bukan sebagai investasi strategis jangka panjang. Kenaikan kembali setelah insiden besar juga menyiratkan respons pembiayaan yang reaktif terhadap krisis, bukan hasil perencanaan *multiyears* yang konsisten.

Komposisi Belanja Pertahanan dan Efek Penggeseran Prioritas (crowding-out)

Kesenjangan pendanaan siber juga perlu dibaca dalam konteks komposisi belanja pertahanan yang masih condong pada biaya personel dan platform konvensional, sementara porsi untuk R&D, C4ISR, serta ranah baru seperti siber relatif terbatas (Hafel & Hi Ibrahim, 2024; Laksmana, 2014). Struktur ini menimbulkan efek penggeseran: program penguatan

arsitektur keamanan jaringan, peningkatan intelijen ancaman, dan pengembangan SDM siber harus bersaing dengan komitmen jangka panjang seperti gaji, pensiun, dan pemeliharaan platform warisan. Bukti internasional menunjukkan bahwa realokasi sebagian kecil anggaran pertahanan ke kapabilitas berkembang dapat memperkuat ketahanan bila diarahkan pada target kemampuan yang jelas dan indikator kinerja yang tepat (Dudzevičiūtė et al., 2021; Dutton et al., 2019).

Transparansi: Agregasi Pos Anggaran dan Konsekuensi Akuntabilitas

Walau reformasi *e-budgeting* dan keterbukaan fiskal telah meningkatkan akuntabilitas di sejumlah sektor (Dewi & Prasojo, 2021; Oktaviani et al., 2019), belanja terkait siber sering muncul dalam label program yang luas dan agregatif (misalnya di BSSN, Kominfo, atau modernisasi pertahanan). Akibatnya, sulit menilai pembagian belanja antara langkah preventif vs reaktif, SDM vs teknologi, serta kebutuhan sipil vs militer. Rendahnya granularitas ini membatasi pengawasan parlemen, lembaga audit, dan masyarakat sipil, sekaligus melemahkan debat berbasis bukti mengenai kecukupan dan efektivitas belanja siber.

Fragmentasi Multi-Aktor dan Dampaknya Pada Pembiayaan

Dinamika pendanaan juga dibentuk oleh fragmentasi kelembagaan: tanggung jawab regulasi dan operasional tersebar di antara BSSN, Kominfo, Kementerian Pertahanan, unit siber TNI, dan regulator sektoral. Literatur menyoroti tumpang tindih mandat, koordinasi lemah, serta penegakan kebijakan yang tidak konsisten (Alfath & Cahya, 2024; Purwandari, 2024). Fragmentasi ini mendorong risiko duplikasi investasi (sistem paralel), inkonsistensi prioritas antar lembaga, dan akuntabilitas yang tidak jelas atas capaian kemampuan siber nasional, sehingga anggaran yang ada tidak selalu terkonversi menjadi kapabilitas terpadu.

Menjawab Rumusan Masalah

Rumusan masalah penelitian ini menanyakan bagaimana prioritas anggaran, pengaturan transparansi, dan praktik kelembagaan membentuk kemampuan Indonesia membiayai pertahanan siber yang efektif. Secara ringkas, hasil menunjukkan tiga mekanisme utama: (i) prioritas fiskal yang masih memusat pada belanja konvensional menyebabkan pendanaan siber kecil dan volatil; (ii) transparansi yang agregatif membatasi evaluasi publik dan mendorong underinvestment; dan (iii) desain institusional yang terfragmentasi melemahkan koordinasi, menimbulkan duplikasi, serta mengurangi efektivitas konversi belanja menjadi kapabilitas. Dengan demikian, penguatan pertahanan siber membutuhkan penataan prioritas, transparansi berjenjang, dan koordinasi lintas lembaga agar retorika sekuritisasi selaras dengan realisasi fiskal.

5. KESIMPULAN DAN SARAN

Berdasarkan sintesis literatur dan data anggaran deskriptif, penelitian ini menunjukkan adanya ketidakseimbangan struktural antara eskalasi ancaman siber dan respons pendanaan serta tata kelola yang tersedia di Indonesia. Ketika insiden siber meningkat dan ketergantungan pada ekonomi digital makin tinggi, alokasi anggaran khusus untuk keamanan siber masih relatif rendah terhadap PDB dan tertinggal dibandingkan beberapa negara tetangga, serta menunjukkan volatilitas yang kuat dari tahun ke tahun, termasuk penurunan tajam pada anggaran BSSN pada 2022.

Pada saat yang sama, peningkatan belanja pertahanan secara total belum otomatis bertransformasi menjadi investasi yang memadai pada domain siber, C4ISR, dan penguatan ketahanan, karena prioritas belanja masih cenderung terpusat pada platform konvensional dan kebutuhan personel (SIPRI Fact Sheet, 2025). Temuan ini juga menegaskan bahwa keterbatasan transparansi yang bersifat agregatif serta fragmentasi kelembagaan antarlembaga membuat pengawasan, evaluasi kinerja, dan konversi belanja menjadi kapabilitas terpadu menjadi lemah. Dengan demikian, pembiayaan pertahanan siber Indonesia, dalam batas bukti yang tersedia pada studi ini, menghadapi empat persoalan utama yang saling terkait, yaitu rendah dan tidak stabilnya alokasi, ketidakselarasan prioritas internal, transparansi dan kerangka kinerja yang lemah, serta fragmentasi institusional yang menghambat koordinasi dan efektivitas capaian.

Sejalan dengan kesimpulan tersebut, penguatan pembiayaan pertahanan siber perlu diarahkan pada konsolidasi kebijakan dan pendanaan yang lebih strategis, terukur, dan berkelanjutan. Pada tingkat pemerintah dan parlemen, disarankan pembentukan program terpadu “Pertahanan Siber dan Ketahanan” dalam APBN yang bersifat multi-tahun agar pendanaan kemampuan inti seperti SOC nasional, perlindungan infrastruktur kritis, respons insiden, serta pengembangan kapasitas dapat berada dalam kerangka koordinasi yang jelas sekaligus meminimalkan duplikasi investasi antar aktor. Selain itu, patokan belanja siber sebagai persentase PDB dapat digunakan sebagai panduan indikatif untuk menaikkan komitmen secara bertahap menuju kisaran 0,05 sampai 0,1 persen, dengan kehati-hatian bahwa target ini bukan kuota kaku dan tetap perlu ditinjau berkala berdasarkan penilaian ancaman, kondisi fiskal, serta bukti efektivitas penggunaan anggaran.

Pada tingkat Kementerian Pertahanan dan TNI, disarankan reorientasi alokasi yang lebih jelas untuk kemampuan siber, komunikasi aman, dan C4ISR, serta integrasi risiko siber ke dalam perencanaan postur, pengadaan, dan evaluasi kesiapan operasional. Ini mencakup penegasan persyaratan keamanan siber pada pengadaan skala besar dan pelibatan elemen siber

dalam latihan serta skenario simulasi secara rutin, sehingga pendanaan siber dapat dipertahankan sebagai kebutuhan kesiapan, bukan sekadar respons teknis.

Pada tingkat BSSN, Kominfo, dan regulator sektoral, disarankan penerapan transparansi berjenjang untuk belanja terkait siber, dengan penyajian informasi publik yang mencakup alokasi agregat, tujuan, dan indikator kinerja, sambil tetap menjaga rincian operasional yang sensitif pada tingkat kerahasiaan yang sesuai. Pendekatan ini diharapkan dapat menyeimbangkan kebutuhan keamanan nasional dan akuntabilitas publik sekaligus memperkuat basis evaluasi berbasis bukti. Selanjutnya, penguatan koordinasi antarlembaga perlu dilembagakan melalui forum perencanaan dan penganggaran bersama, termasuk protokol respons insiden terpadu dan rencana investasi bersama untuk infrastruktur seperti SOC, CERT, dan pusat pelatihan, serta mengaitkan persetujuan anggaran dengan bukti koordinasi lintas institusi untuk menekan fragmentasi dan meningkatkan efektivitas belanja.

Keterbatasan penelitian ini perlu dicatat secara terbuka agar rekomendasi dipahami secara proporsional. Studi ini menggunakan tinjauan literatur kualitatif non-sistematis dan data anggaran deskriptif yang bergantung pada dokumen publik dan estimasi sekunder pada sektor yang historis minim transparansi, sehingga angka-angka anggaran serta proporsi belanja terhadap PDB sebaiknya dipandang indikatif. Selain itu, penelitian ini tidak menggunakan model statistik formal sehingga tidak mendukung inferensi kausal yang kuat, dan analisis tata kelola kelembagaan bergantung pada sumber sekunder tanpa wawancara primer sehingga berpotensi belum menangkap dinamika internal maupun praktik informal.

Untuk penelitian selanjutnya, disarankan penggunaan metode campuran yang mengombinasikan pelacakan anggaran rinci, wawancara pemangku kepentingan kunci, dan studi kasus insiden siber untuk memperdalam pemahaman tentang proses negosiasi dan implementasi anggaran. Pengembangan klasifikasi standar belanja siber lintas lembaga juga penting agar monitoring konsisten dari waktu ke waktu, sekaligus membuka ruang bagi analisis kuantitatif seperti deret waktu atau simulasi untuk menilai dampak variasi komposisi belanja terhadap ketahanan. Studi komparatif sektoral pada infrastruktur kritis seperti energi, kesehatan, keuangan, dan pemilu juga dapat membantu menunjukkan bagaimana keputusan pendanaan diterjemahkan menjadi kapabilitas nyata dan bagaimana posisi Indonesia dibanding negara berpendapatan menengah lain dengan tantangan serupa.

DAFTAR REFERENSI

Acosta, M., Coronado, D., Ferrandiz, E., Marin, M. R., & Moreno, P. J. (2018). Patents and dual-use technology: An empirical study of the world's largest defence companies. *Defence and Peace Economics*, 29(7), 821–839. https://doi.org/10.1080/10242694.2017.1303239

Alfath, T. P., & Cahya, W. (2024). Bridging the gap between policy and practice: Evaluating Indonesia's cybersecurity regulatory framework (2020–2023). *Data*, 2(1), 14–24. https://doi.org/10.61978/data.v2i1.695

APBN Kita: Kinerja dan fakta. (2022). *Direktorat Jenderal Anggaran*. https://djpk.kemenkeu.go.id/wp-content/uploads/2022/12/V-Final-Publikasi-APBN-KiTa-Ed-Desember-2022.pdf

Bogdanoski, M., & Nikolov, E. (2007). *Dual-use and conversion of military-related R&D in Germany*. https://eprints.ugd.edu.mk/8837/

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers. https://doi.org/10.1515/9781685853808

Challenges to effective EU cybersecurity policy (Briefing paper). (2019). *European Court of Auditors*. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

Dewi, S. P. P., & Prasojo, E. (2021). The impact of state budget transparency and information dissemination to maintain public trust. *J. Natapraja: Kajian Ilmu Administrasi Negara*, 9(2). https://doi.org/10.21831/natapraja.v9i2.40474

Dudzevičiūtė, G., Bekešienė, S., Meidutė-Kavaliauskienė, I., & Ševčenko-Kozlovska, G. (2021). An assessment of the relationship between defence expenditure and sustainable development in the Baltic countries. *Sustainability*, 13(12). https://doi.org/10.3390/su13126916

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity capacity: Does it matter? *Journal of Information Policy*, 9, 280–306. https://doi.org/10.5325/jinfopoli.9.2019.0280

Fatihah, C. Y. N. (2021). Establishing a legitimate Indonesia's government electronic surveillance regulation: A comparison with the U.S. legal practices. *Indonesia Law Review*, 11(3), 323–336. https://doi.org/10.15742/ilrev.v11n3.6

Hafel, M., & Hi Ibrahim, A. H. (2024). Budget politics in Indonesia: Processes, challenges, and economic implications. *International Research Journal of Management, IT and Social Sciences*, 11(4), 159–168. https://doi.org/10.21744/irjmis.v11n4.2457

Khaw, T. Y., Amran, A., & Teoh, A. P. (2024). Building a thematic framework of cybersecurity: A systematic literature review approach. *Journal of Systems and Information Technology*, 26(2), 234–256. https://doi.org/10.1108/JSIT-07-2023-0132

Laksmana, E. A. (2014). The hidden challenges of Indonesia's defence modernisation. *Indonesian Defence*, 34(3), 17–19.

Lambert, V. A., & Lambert, C. E. (2012). Qualitative descriptive research: An acceptable design. *Pacific Rim International Journal of Nursing Research*, 16(4), 255–256.

Lu, W.-M., Kweh, Q. L., Nourani, M., & Huang, F.-W. (2016). Evaluating the efficiency of dual-use technology development programs from the R&D and socio-economic perspectives. *Omega*, 62, 82–92. https://doi.org/10.1016/j.omega.2015.08.011

Marwan, A., & Bonfigli, F. (2022). Detection of digital law issues and implication for good governance policy in Indonesia. *Bestuur*, 10(1), 22–32. https://doi.org/10.20961/bestuur.v10i1.59143

Meidyasari, S. (2024). The impact of digital economy in driving economic growth and development in Indonesia. *INJURITY: Journal of Interdisciplinary Studies*, 3(11), 777–783. https://doi.org/10.58631/injurity.v3i11.1306

Nozadze, M. (2018). *The impact of military tension on economic growth: Comparative study of Israel and South Korea*.

OECD. (2017). *OECD budget transparency toolkit*. Organisation for Economic Co-operation and Development. https://doi.org/10.1787/9789264282070-en

Oktaviani, R. F., Puspaningtyasfaeni, D., & Puspitaningtyasfaeni, R. (2019). E-budgeting for public finance transparency and accountability. *International Journal of Recent Technology and Engineering*, 8(2S4), 854–857. https://doi.org/10.35940/ijrte.B1170.0782S419

Otukoya, T. A. (2024). The securitization theory. *International Journal of Science and Research Archive*, 11(1), 1747–1755. https://doi.org/10.30574/IJSRA.2024.11.1.0225

Primawanti, H., Wibowo, S. E., Hartono, A., Kiswanto, H., & Louerens, J. T. A. (2024). Securitization of cyber threats to the Indonesian government: A study of cyber defense strategy. *GPS Journal*, 8(2), 97–108. https://doi.org/10.34010/gpsjournal.v8i2.13817

Purwandari, N. (2024). Cybersecurity challenges and investment in Indonesia. *Data*, 2(2), 85–92. https://doi.org/10.61978/data.v2i2.696

Putra, B. R., Yeniwati, Y., & Adry, M. R. (2019). Analisis kausalitas belanja pertahanan dan pertumbuhan ekonomi di Indonesia. *Ecosains*, 8(2), 177. https://doi.org/10.24036/ecosains.11524357.00

Ringkasan rencana kerja dan anggaran BSSN tahun anggaran 2023. (2023). *Badan Anggaran DPR RI*.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors*, 23(15), 6666. https://doi.org/10.3390/s23156666

Salahudin, S., Sihidi, I. T., Karida, K., & Firdaus, M. (2024). Digital budgeting transformation and future challenges: A bibliometric analysis. *Journal of Government and Public Policy*, 11(3), 257–270. https://doi.org/10.18196/jgpp.v11i3.21182

Sandelowski, M. (2000). Whatever happened to qualitative description? *Research in Nursing & Health*, 23(4), 334–340. https://doi.org/10.1002/1098-240X(200008)23:4<334::AID-NUR9>3.0.CO;2-G

Saputro, G. E., Rivai, A. M., & Meirinaldi, M. (2021). Pengaruh anggaran pertahanan, impor alutsista, ekspor alutsista, dan inflasi terhadap pertumbuhan ekonomi di Indonesia tahun 1980–2019. *Jurnal Ekonomi*, 23(2), 103–115. https://doi.org/10.37721/je.v23i2.801

SIPRI fact sheet. (2025). *Stockholm International Peace Research Institute*.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Soelistyo, A. (2023). How strongly does military expenditure impact economic growth and the exchange rate? *Jurnal Ilmiah Bisnis dan Ekonomi Asia*, 17(3), 266–278. https://doi.org/10.32815/jibeka.v17i3.1177

Solanki, S., Paluri, A. R., & Singh, S. (2023). Exploring the dynamics of defense expenditure and economic development: A bibliometric analysis. *International Journal of Business and Society*, 24(3), 1314–1343. https://doi.org/10.33736/ijbs.6423.2023