DAMPAK MASUKNYA STARLINK KE INDONESIA TERHADAP KEAMANAN JARINGAN NASIONAL DENGAN METODE SLR (SYSTEMATICS LITERATURE REVIEW)

Rahmat Rambe[1,*], Fairuz Fernanda Hermawan[2], Rd. Rohmat Saedudin[3]

[1,2,3] *Jurusan Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom, Bandung,*

Abstrak

Penelitian ini bertujuan untuk menganalisis dampak masuknya layanan internet satelit Starlink terhadap keamanan jaringan nasional Indonesia melalui pendekatan *Systematic Literature Review (SLR)* berbasis panduan PRISMA 2020. Sebanyak 34 artikel ilmiah dari tahun 2020–2024 diseleksi menggunakan kriteria inklusi-eksklusi yang ketat dan dianalisis menggunakan pendekatan sintesis tematik. Tiga tema utama ditemukan: (1) peningkatan kerentanan terhadap serangan siber akibat karakteristik arsitektur satelit; (2) ketimpangan kesiapan regulasi dan pengawasan hukum di negara berkembang; serta (3) kebutuhan kolaborasi nasional dalam membangun pertahanan siber berbasis kebijakan lokal. Studi ini memberikan kontribusi pada literatur mengenai keamanan infrastruktur digital di Indonesia dan mengusulkan kerangka kebijakan nasional untuk mengantisipasi masuknya teknologi global seperti Starlink. Penelitian ini menekankan pentingnya integrasi antara regulasi, teknologi, dan aktor nasional untuk memastikan kedaulatan digital Indonesia.

Kata Kunci:
Starlink, Keamanan Jaringan Nasional, Review Literasi Sistematik, Jaringan Satelit, Regulasi Kebijakan Keamanan.

Abstract

This study aims to analyze the impact of the entry of Starlink satellite internet services on Indonesia's national network security through a Systematic Literature Review (SLR) approach based on the PRISMA 2020 guidelines. A total of 34 scientific articles from 2020–2024 were selected using strict inclusion-exclusion criteria and analyzed using a thematic synthesis approach. Three main themes were found: (1) increased vulnerability to cyber attacks due to satellite architecture characteristics; (2) inequality in regulatory readiness and legal oversight in developing countries; and (3) the need for national collaboration in building local policy-based cyber defense. This study contributes to the literature on digital infrastructure security in Indonesia and proposes a national policy framework to anticipate the entry of global technologies such as Starlink. This study emphasizes the importance of integration between regulation, technology, and national actors to ensure Indonesia's digital sovereignty.

Keywords:
Starlink, National Network Security, Systematic Literature Review (SLR), Satellite Networks, Security Policy Regulation

1. PENDAHULUAN

Perkembangan teknologi komunikasi melalui satelit telah mendorong terciptanya solusi inovatif untuk mengatasi kesenjangan konektivitas global. Salah satu inovasi terkemuka dalam bidang ini adalah Starlink, proyek ambisius dari SpaceX yang bertujuan menyediakan layanan internet global berkecepatan tinggi melalui konstelasi ribuan satelit orbit rendah (LEO). Starlink menjanjikan akses internet yang cepat dan stabil, terutama di wilayah-wilayah yang belum terjangkau oleh infrastruktur jaringan terestrial tradisional. Di Indonesia, yang memiliki tantangan geografis sebagai negara kepulauan, teknologi ini menawarkan potensi strategis dalam menjembatani kesenjangan digital antarwilayah.

Dengan kapabilitas untuk menjangkau wilayah-wilayah terpencil yang sulit dilalui oleh jaringan serat optik maupun menara telekomunikasi (Khaliq, Rakib, dan Aris 2024), Starlink hadir sebagai pilihan yang sangat relevan dalam mendukung pembangunan infrastruktur digital nasional. Teknologi ini juga memiliki potensi besar untuk mempercepat pemerataan akses terhadap pendidikan, layanan kesehatan,

* Korespondensi
E-mail: gyurahmat@student.telkomuniversity.ac.id

dan peluang ekonomi berbasis digital di kawasan 3T (tertinggal, terdepan, dan terluar). Selain itu, pemanfaatan Starlink sejalan dengan arah kebijakan pemerintah dalam mewujudkan transformasi digital, khususnya dalam memperkuat sistem informasi dan komunikasi nasional di tengah situasi global yang semakin dinamis dan kompleks (Hukunala 2024). Meski demikian, pelaksanaan teknologi ini tetap membutuhkan telaah terhadap kerangka regulasi, perlindungan terhadap keamanan siber, serta aspek keberlanjutan, agar manfaatnya dapat dirasakan secara menyeluruh dan berkesinambungan oleh seluruh lapisan masyarakat (Nudan, Widodo, dan Affifudin 2024).

Meski demikian, kehadiran teknologi luar negeri yang bersifat transnasional seperti Starlink membawa persoalan baru, khususnya dalam aspek keamanan jaringan nasional,kedaulatan data, dan regulasi kebijakan digital (Tedeschi, Sciancalepore, dan Di Pietro 2022). Ketersediaan akses langsung dari konsumen ke satelit (Direct-to-User Access) tanpa keterlibatan penuh otoritas nasional memicu kekhawatiran atas kendali data dan potensi intervensi eksternal dalam infrastruktur digital Indonesia. Ancaman ini tidak hanya bersifat teknis seperti serangan Distributed Denial of Service (DDoS), packet sniffing, dan DNS hijacking, tetapi juga menyangkut aspek hukum, sosial, dan geopolitik yang belum sepenuhnya terfasilitasi oleh kebijakan nasional (Garcia-Cabeza dkk. 2025).

Absennya mekanisme pengawasan nasional yang efektif terhadap pergerakan data lintas batas meningkatkan risiko terjadinya pelanggaran terhadap hak privasi masyarakat. Selain itu, masuknya teknologi luar tanpa proses integrasi dengan sistem digital domestik berpotensi menurunkan daya saing penyedia layanan lokal dan memperkuat ketergantungan pada aktor global yang sulit dijangkau oleh regulasi nasional (Coche, Kolk, dan Ocelík 2024). Dalam ranah geopolitik, penguasaan infrastruktur komunikasi oleh pihak asing juga bisa menjadi pintu masuk bagi intervensi politik luar negeri yang tidak sejalan dengan kepentingan nasional. Oleh karena itu, dibutuhkan perumusan kebijakan yang responsif, inklusif, dan berlandaskan pada prinsip kedaulatan digital untuk mengelola operasional layanan satelit asing tanpa menghambat perkembangan teknologi serta keterbukaan akses informasi (Boeira dkk. 2023).

Sistem komunikasi satelit LEO rentan terhadap berbagai serangan siber karena karakteristiknya yang mobile, terbuka, dan beroperasi lintas negara (Yue dkk. 2022). Ancaman ini semakin nyata jika negara tujuan tidak memiliki regulasi atau infrastruktur teknis yang mampu menanggulangi risiko dari luar. Dalam konteks Indonesia, yang baru menyusun kebijakan perlindungan data melalui UU No. 27 Tahun 2022, masih terdapat kesenjangan besar dalam kesiapan pengawasan teknologi seperti Starlink yang dapat menyalurkan dan menyimpan data di luar negeri .

Kerawanan ini semakin meningkat karena belum tersedianya sistem deteksi dini dan respons insiden yang terkoordinasi secara nasional untuk jaringan berbasis luar angkasa, termasuk sistem enkripsi dan pemantauan lintas batas negara dalam transmisi data. Di sisi lain, struktur desentralisasi pada sistem Starlink menyulitkan upaya pelacakan serta pelaporan ketika terjadi kebocoran atau penyadapan informasi (Sitouah, Merazka, dan Hedjazi 2022). Kondisi ini menciptakan tantangan besar bagi lembaga perlindungan data nasional dalam menjamin bahwa data strategis milik warga negara tidak dimanfaatkan oleh entitas asing. Di samping itu, kekurangan tenaga ahli yang memahami seluk-beluk keamanan siber satelit memperumit upaya penegakan kedaulatan digital di tingkat nasional (Kwentoa 2025). Ketidakseimbangan ini membuka peluang bagi masuknya pengaruh teknologi asing yang tidak tunduk langsung pada sistem hukum nasional, yang pada akhirnya bisa mengancam kestabilan informasi dan menurunkan tingkat kepercayaan publik terhadap sistem komunikasi negara (Roberts 2024).

Kajian sebelumnya banyak berfokus pada performa teknis Starlink, seperti kecepatan, latensi, dan arsitektur jaringan (Michel 2022), namun belum ditemukan studi yang secara khusus mengkaji secara sistematis implikasi kehadiran Starlink terhadap keamanan jaringan nasional Indonesia (Pan 2023). Di sisi lain, studi-studi kebijakan yang dilakukan di negara-negara Asia Tenggara seperti Thailand menekankan pentingnya kesiapan regulasi dan kontrol nasional dalam menjaga keseimbangan antara inovasi dan keamanan nasional (Shaengchart dan Kraiwanit 2024) .

Oleh karena itu, penelitian ini disusun dengan pendekatan Systematic Literature Review (SLR) berdasarkan panduan PRISMA 2020, dengan tujuan mengidentifikasi, mengevaluasi, dan mensintesis literatur akademik yang relevan mengenai dampak kehadiran Starlink terhadap keamanan jaringan nasional. Penelitian ini juga menggunakan pendekatan sintesis tematik untuk mengeksplorasi secara mendalam isu-isu strategis, teknis, dan regulatif yang dihadapi oleh Indonesia dalam mengelola infrastruktur berbasis satelit yang dikendalikan oleh entitas asing.

2. TINJAUAN PUSTAKA

Untuk menilai kesiapan nasional dalam menghadapi risiko keamanan dari teknologi komunikasi luar negeri, penelitian ini merujuk pada NIST Cybersecurity Framework (CSF). Kerangka ini terbagi ke dalam lima fungsi utama: identifikasi, proteksi, deteksi, respons, dan pemulihan. Dalam konteks Indonesia, berdasarkan laporan Global Cybersecurity Index (GCI) oleh ITU tahun 2021, Indonesia berada pada posisi ke-24 dari 194 negara, dan peringkat ke-5 di ASEAN, yang menunjukkan bahwa meskipun terdapat kemajuan, masih diperlukan penguatan pada dimensi organisasi dan teknis (Putro 2023).

Hal ini menunjukkan bahwa walaupun Indonesia telah melakukan berbagai langkah signifikan dalam merancang kebijakan serta membangun infrastruktur keamanan siber, implementasi tersebut belum sepenuhnya mencakup seluruh sektor strategis yang rentan terhadap serangan digital lintas batas negara(Irawan Hafizhan, Muhammad Alva Hendi, dan Nasiri Asro 2024). Permasalahan utama berada pada belum terjalinnya sinergi yang kuat antarinstansi, terbatasnya jumlah tenaga profesional di bidang keamanan siber, serta penerapan standar proteksi yang masih belum maksimal dalam sistem komunikasi nasional(Indirwan dan Aulianisa 2020). Oleh sebab itu, pemanfaatan NIST CSF bukan sekadar sebagai panduan teoretis, melainkan juga harus menjadi dasar dalam melakukan penilaian berkala dan peningkatan kapasitas teknis secara menyeluruh, agar Indonesia dapat secara tangguh menghadapi dan merespons ancaman keamanan digital dari teknologi asing (Ghozie Afiansyah, Annisa, dan Febriyani 2023).

Kerangka NIST juga digunakan untuk mengevaluasi bagaimana risiko dari teknologi LEO seperti Starlink dapat dikenali lebih awal, dilindungi dari serangan aktif, dan ditangani secara strategis oleh lembaga seperti Badan Siber dan Sandi Negara (BSSN). Fungsi-fungsi ini sangat relevan dalam menganalisis kesiapan lembaga nasional untuk menanggulangi ancaman sistemik dari penyedia layanan global (Bakyt dkk. 2025).

Dalam konteks ini, penerapan kerangka kerja NIST tidak hanya berfungsi sebagai perangkat teknis, tetapi juga sebagai mekanisme koordinatif yang mendukung terciptanya interoperabilitas antara lembaga pemerintah, sektor privat, dan pelaku lintas batas negara (Tanjung, Dwi Nurhayati, dan Wibowo 2024). Aspek ini menjadi sangat penting karena teknologi LEO memiliki sifat lintas yurisdiksi dan relatif sulit dikontrol oleh kebijakan regulasi yang bersifat tradisional, sehingga dibutuhkan strategi yang bersifat multidimensi yang mengacu pada standar internasional namun tetap menjunjung tinggi prinsip kedaulatan digital nasional (Credi dan Vianini 2021).

Kedaulatan digital mengacu pada hak eksklusif negara dalam mengatur, mengakses, dan melindungi data warganya. Starlink, sebagai penyedia layanan berbasis satelit lintas batas, secara langsung menghadirkan risiko terhadap prinsip data sovereignty karena tidak semua lalu lintas data dapat dikendalikan atau dipantau oleh otoritas Indonesia. Kajian oleh menunjukkan bahwa tanpa regulasi yang mengatur alur data secara tegas, negara berkembang rentan terhadap dominasi digital dari perusahaan asing yang dapat menyalahgunakan posisi pasar mereka (Priyanka 2021).

Kondisi ini menjadi semakin rumit karena infrastruktur satelit orbit rendah seperti Starlink dapat beroperasi secara lintas negara tanpa kehadiran fisik di wilayah hukum negara pengguna, yang pada akhirnya menciptakan celah dalam yurisdiksi nasional dan memungkinkan penghindaran terhadap kewajiban pelaksanaan regulasi perlindungan data di tingkat domestik (Ortiz dkk. 2024). Oleh sebab itu, Indonesia tidak hanya perlu menyusun aturan yang bersifat teknis, tetapi juga harus membangun kerangka diplomasi digital yang kokoh untuk memperkuat posisi tawar dalam forum internasional terkait tata kelola ruang siber dan arus data lintas batas (Darmayadi dkk. 2025).

Pemerintah Indonesia melalui UU No. 27 Tahun 2022 dan UU No. 36 Tahun 1999 memang telah menetapkan perlindungan data sebagai hak dasar, namun hingga saat ini belum terdapat mekanisme teknis dan peraturan pelaksana yang menjamin kepatuhan penyedia satelit asing seperti Starlink terhadap prinsip-prinsip tersebut.

Karakteristik infrastruktur LEO seperti Starlink meliputi koneksi antar-satelit (inter-satellite links), mobilitas tinggi, dan jangkauan luas, namun justru inilah yang menambah kerentanan terhadap serangan. dalam penelitiannya mengidentifikasi beberapa potensi ancaman pada terminal Starlink, termasuk remote hijacking, DNS spoofing, dan eksploitasi pada lapisan aplikasi (Peled dkk. 2023). Starlink menghadirkan tantangan tersendiri karena ia menciptakan "jaringan dalam jaringan" yang tidak terintegrasi dengan sistem pengawasan nasional (Kareem t.t.).

Selain itu, fleksibilitas Starlink dalam mengalihkan lalu lintas data secara dinamis melalui jaringan satelit tanpa ketergantungan pada infrastruktur berbasis darat menambah tingkat kerumitan dalam proses pemantauan trafik digital (Westphal, Han, dan Li 2023). Kondisi ini tidak hanya mempersulit identifikasi awal terhadap potensi intrusi, tetapi juga menyebabkan atribusi terhadap serangan siber menjadi kabur

karena jalur transmisi informasi yang tidak transparan dan sulit untuk dipantau secara langsung oleh aparat keamanan siber nasional (Ma dkk. 2024).

Tingkat latensi dan packet loss pada jaringan Starlink cenderung fluktuatif dan lebih rentan terhadap interferensi luar, terutama di wilayah dengan kepadatan satelit rendah seperti Asia Tenggara(Yue dkk. 2022). Faktor-faktor seperti kondisi atmosfer di wilayah tropis, kendala topografi, serta belum memadainya infrastruktur penunjang di daratan turut memperburuk kestabilan kinerja jaringan di wilayah ini. Selain itu, keterbatasan jumlah stasiun bumi regional dan lemahnya koordinasi dalam pengelolaan spektrum frekuensi di level kawasan ikut meningkatkan potensi gangguan konektivitas serta mengurangi efektivitas layanan ketika terjadi lonjakan lalu lintas data secara mendadak (Shukur dkk. 2025).

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan *Systematic Literature Review (SLR)* yang disusun berdasarkan pedoman PRISMA *(Preferred Reporting Items for Systematic Reviews and Meta-Analyses)* tahun 2020, yang dirancang untuk mendukung proses peninjauan literatur secara transparan, terstruktur, dan berulang. Pendekatan ini dipilih karena kemampuannya dalam menjawab pertanyaan penelitian yang kompleks dan multidimensi, khususnya yang menyangkut teknologi lintas batas, seperti Starlink, yang dampaknya tidak hanya bersifat teknis, tetapi juga berkaitan erat dengan hukum, kebijakan, dan keamanan nasional. Melalui SLR, penelitian ini bertujuan untuk menyusun pemahaman yang menyeluruh dan berbasis bukti mengenai potensi risiko dan peluang dari hadirnya layanan internet satelit orbit rendah terhadap infrastruktur dan keamanan jaringan nasional Indonesia.

Proses SLR ini dimulai dengan perumusan fokus kajian melalui pertanyaan penelitian utama, yakni: Bagaimana kehadiran Starlink sebagai penyedia layanan satelit LEO memengaruhi keamanan jaringan nasional Indonesia, baik dari aspek teknis, regulatif, maupun kedaulatan digital?" Pertanyaan ini kemudian mengarahkan strategi pencarian literatur, penyaringan sumber, dan kerangka penyusunan sintesis tematik yang digunakan dalam analisis.

Pencarian literatur dilakukan melalui beberapa basis data akademik terkemuka, antara lain Scopus, IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, serta Google Scholar sebagai pelengkap. Pemilihan database tersebut didasarkan pada kelengkapan indeksasi, cakupan multidisiplin, dan reputasi internasional. Proses pencarian dilakukan pada periode Mei hingga Juni 2024 menggunakan kata kunci kombinatif yang relevan, termasuk: “Starlink”, “LEO satellite internet”, “cybersecurity”, “national network security”, “data sovereignty”, “Indonesia”, “developing countries”, dan “regulatory framework.” Operator boolean digunakan untuk memperluas atau mempersempit hasil pencarian agar tepat sasaran.

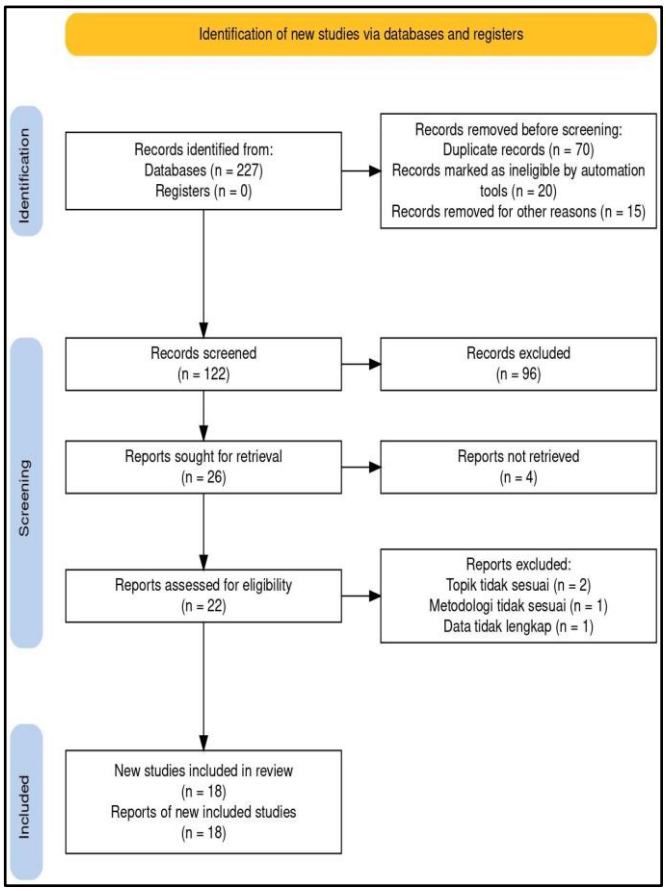
Batasan inklusi dalam pencarian mencakup artikel jurnal ilmiah yang telah melalui proses peer-review, diterbitkan dalam rentang waktu tahun 2020 hingga 2024, serta ditulis dalam bahasa Inggris. Artikel yang diterima adalah studi yang secara eksplisit membahas Starlink atau teknologi serupa, dengan fokus pada dampak keamanan jaringan, kebijakan digital, atau isu kedaulatan data di negara-negara berkembang, khususnya Indonesia dan kawasan Asia Tenggara. Sementara itu, artikel eksklusif berupa opini populer, berita media massa, blog, laporan perusahaan, serta publikasi yang tidak dapat diakses secara penuh dikeluarkan dari daftar. Studi yang hanya membahas performa teknis seperti kecepatan atau latensi tanpa mengaitkan pada aspek kebijakan atau keamanan juga dikecualikan, karena dianggap tidak memenuhi kerangka kajian tematik.

Tahapan seleksi dilakukan secara sistematis dan bertahap. Dari total 227 artikel yang teridentifikasi dalam tahap awal, dilakukan proses penghilangan duplikasi dan penyaringan awal berdasarkan judul dan abstrak. Hasilnya, sebanyak 122 artikel melanjutkan ke tahap evaluasi mendalam. Setelah dikaji isi dan relevansinya dengan fokus penelitian, diperoleh 18 artikel akhir yang digunakan dalam analisis. Seluruh proses ini mengikuti alur PRISMA yang mencakup empat tahap utama: identifikasi, penyaringan, penilaian kelayakan, dan inklusi akhir. Diagram PRISMA secara visual menggambarkan alur keputusan pada tiap tahap seleksi dan menjadi alat bantu yang memastikan proses dilakukan secara replikatif dan terbuka.

Seluruh artikel yang lolos seleksi kemudian diekstraksi datanya secara manual dan digital menggunakan bantuan perangkat lunak Zotero untuk manajemen referensi serta Microsoft Excel untuk mengklasifikasikan temuan. Setiap artikel dianalisis berdasarkan identitas publikasi, tujuan penelitian, konteks geografis, fokus utama, serta temuan yang relevan dengan tema penelitian. Selanjutnya, proses pengelompokan tema dilakukan melalui sintesis tematik (thematic synthesis), yang merupakan metode kualitatif dalam menafsirkan hasil dari studi-studi sebelumnya ke dalam tema-tema baru yang lebih tinggi tingkat abstraksinya.

Sintesis tematik dalam studi ini disusun berdasarkan lima tahapan. Tahap pertama adalah membaca dan memahami keseluruhan artikel secara komprehensif. Selanjutnya dilakukan proses pengkodean awal

(initial coding) untuk menandai konsep-konsep utama yang berulang. Kode-kode ini lalu dikelompokkan ke dalam sub-tema berdasarkan kemiripan makna, dan dari sana dikembangkan menjadi tema utama yang mencerminkan struktur naratif dari data literatur. Pada tahap akhir, masing-masing tema ditelaah kembali dengan memperhatikan konteks Indonesia, serta disusun dalam bentuk narasi yang mengaitkan antar-tema secara logis .



Gambar 1. Alur SLR

Hasil dari proses sintesis ini menghasilkan tiga tema utama: pertama, meningkatnya kerentanan teknis terhadap serangan siber akibat karakteristik unik dari infrastruktur satelit LEO; kedua, ketimpangan regulatif dan lemahnya pengawasan hukum terhadap entitas asing yang beroperasi di luar yurisdiksi nasional; dan ketiga, ancaman terhadap kedaulatan digital dan kontrol atas data nasional, terutama dalam konteks arsitektur Starlink yang memungkinkan transfer data langsung ke luar negeri tanpa otorisasi lokal. Di luar tema utama, terdapat dua temuan tambahan yang muncul secara konsisten yaitu urgensi kolaborasi lintas sektor dalam penguatan keamanan siber nasional, serta perbandingan lintas negara dalam menyikapi hadirnya teknologi LEO sebagai instrumen geopolitik digital (Zhang dkk. 2025).

Validitas proses SLR ini dijaga melalui penelaahan silang oleh dua peneliti secara independen. Ketidaksesuaian dalam proses seleksi maupun pengkodean diselesaikan melalui diskusi bersama hingga tercapai konsensus. Setiap tahapan dokumentasi dari identifikasi hingga sintesis disimpan dan dapat diaudit ulang sebagai bentuk akuntabilitas ilmiah. Dengan demikian, metode penelitian ini tidak hanya menjawab pertanyaan riset dengan kedalaman konseptual, tetapi juga memberikan kontribusi metodologis dalam bentuk praktik tinjauan literatur yang dapat direplikasi dan diverifikasi oleh peneliti lain dalam bidang serupa.

4. HASIL DAN PEMBAHASAN

Hasil kajian literatur yang telah dianalisis melalui pendekatan sintesis tematik menghasilkan tiga tema utama yang saling berkaitan, yaitu: (1) kerentanan infrastruktur jaringan satelit terhadap ancaman siber, (2) ketimpangan kesiapan regulasi nasional dalam menghadapi penyedia layanan global, serta (3) ancaman terhadap kedaulatan digital dan kontrol atas data. Selain itu, terdapat dua tema tambahan yang juga mengemuka secara konsisten dalam literatur, yaitu kebutuhan kolaborasi lintas sektor nasional serta pembelajaran dari pendekatan negara lain di Asia dan Afrika terhadap layanan Starlink.

1. Kerentanan Infrastruktur Satelit terhadap Ancaman Siber

Tema pertama yang muncul secara dominan dalam literatur adalah tingginya kerentanan jaringan satelit LEO, seperti Starlink, terhadap berbagai bentuk serangan siber. Karakteristik sistem Starlink yang terdiri atas ribuan satelit bergerak dengan inter-satellite links (ISLs) menyebabkan dinamika koneksi yang lebih kompleks dibandingkan dengan jaringan terestrial konvensional. Satelit LEO cenderung menghadapi risiko tinggi terhadap jamming, spoofing, man-in-the-middle attacks, serta denial of service (DoS), terutama ketika tidak didukung oleh sistem enkripsi yang kuat dan perangkat deteksi dini (Kareem t.t.; Yue dkk. 2022).

Starlink memiliki celah keamanan yang memungkinkan serangan dari dalam jaringan lokal. Kerentanan ini diperburuk oleh fakta bahwa layanan ini beroperasi di luar pengawasan infrastruktur jaringan domestik, sehingga mekanisme pertahanan jaringan nasional tidak dapat berfungsi secara penuh. Dalam konteks Indonesia, di mana masih terdapat kelemahan dalam integrasi sistem keamanan antarinstansi (BSSN, Kominfo, operator), celah ini dapat menjadi titik masuk bagi ancaman siber berskala nasional (Peled dkk. 2023).

Infrastruktur satelit digunakan secara masif tanpa mitigasi lokal, hal tersebut dapat meningkatkan attack surface nasional yang sebelumnya terkonsentrasi pada jaringan terestrial. Dalam konteks Indonesia, hal ini berarti Starlink dapat memperbesar potensi risiko serangan tanpa kontribusi langsung terhadap sistem keamanan domestik, karena keterpisahan fisik dan yuridis dari infrastruktur nasional (Ogutu dan Oughton 2021).

2. Ketimpangan Regulasi Nasional terhadap Entitas Luar Negeri

Tema kedua yang sangat penting adalah ketidakseimbangan antara regulasi nasional dengan sifat operasi global dari layanan seperti Starlink. Sebagian besar literatur menunjukkan bahwa banyak negara berkembang, termasuk Indonesia, belum memiliki kerangka hukum yang memadai untuk mengatur entitas luar negeri yang menawarkan layanan telekomunikasi secara langsung kepada konsumen lokal. Dalam hal ini, Starlink mendapatkan dua izin penting di Indonesia pada 2024, yakni izin sebagai Internet Service Provider (ISP) dan penyelenggara VSAT, namun belum terdapat mekanisme konkret yang memastikan keterlibatan penuh pemerintah dalam pengawasan teknis maupun alur data.

Penyedia satelit global dapat menghindari beban regulatif dengan memanfaatkan celah hukum yang tidak secara eksplisit melarang atau membatasi operasi satelit asing. Kondisi serupa berpotensi terjadi di Indonesia apabila revisi terhadap UU Telekomunikasi dan UU PDP tidak segera dilengkapi dengan regulasi turunan yang mengatur spesifik tentang satelit orbit rendah dan hak negara atas pengendalian jaringan (Shaengchart dan Kraiwanit 2024).

Literatur juga menyoroti tantangan dalam menjamin compliance terhadap standar lokal oleh perusahaan global seperti Starlink. Meskipun negara memiliki wewenang hukum atas spektrum frekuensi dan izin operasi, namun pelaksanaan pengawasan dan audit teknis masih sangat lemah, terutama jika penyedia tidak membangun titik interkoneksi fisik di dalam negeri (Priyanka 2021).

Dalam konteks Indonesia, ketimpangan ini diperkuat oleh keterbatasan kapasitas teknis institusi pengawas serta belum optimalnya kolaborasi antara lembaga regulatif, operator lokal, dan komunitas teknis. Hal ini menimbulkan risiko bahwa Starlink akan menjadi entitas yang beroperasi secara extraterritorial menghubungkan konsumen Indonesia langsung ke jaringan luar tanpa pengawasan atau keterlibatan nasional.

3. Ancaman terhadap Kedaulatan Digital dan Pengendalian Data

Tema ketiga yang muncul sebagai benang merah dari berbagai artikel adalah ancaman terhadap kedaulatan digital. Starlink, dengan arsitektur jaringannya yang mengalirkan data langsung ke gateway internasional, membuka ruang bagi pelanggaran prinsip data sovereignty. Negara yang tidak memiliki

kontrol atas penyimpanan, aliran, dan pemrosesan data secara domestik berpotensi kehilangan kendali atas informasi strategis, termasuk data pribadi, komunikasi publik, dan lalu lintas komersial.

Negara-negara yang tidak memiliki data localization policy akan kesulitan menegakkan yurisdiksi digital atas penyedia seperti Starlink. Di Indonesia, meskipun terdapat UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, masih belum tersedia infrastruktur dan regulasi yang mampu menegakkan prinsip tersebut dalam konteks teknologi satelit. Hal ini menjadi celah besar yang dapat dimanfaatkan oleh pihak asing untuk menyimpan atau mengalihkan data warga negara ke luar negeri tanpa izin eksplisit atau pemantauan local (Monash Hub 2024; Putro 2023).

Literatur juga menyoroti potensi disrupsi terhadap model bisnis penyedia lokal akibat tidak setaranya kewajiban antara entitas asing dan domestik. Sementara ISP lokal wajib menyediakan pusat data, audit kepatuhan, dan sertifikasi keamanan, penyedia seperti Starlink dapat mengoperasikan layanannya tanpa persyaratan teknis yang setara, menciptakan ketimpangan struktural dalam ekosistem digital nasional.

Pentingnya kolaborasi antara pemerintah, penyedia layanan, dan komunitas siber dalam menciptakan strategi pertahanan yang adaptif. Kolaborasi ini tidak hanya bersifat teknis, tetapi juga menyangkut edukasi publik, standarisasi peralatan, dan peningkatan kapasitas sumber daya manusia dalam mengelola risiko dari teknologi satelit (Dinis 2022; Kassem 2022).

Upaya ini menjadi semakin penting mengingat semakin besarnya ketergantungan publik terhadap infrastruktur digital yang secara langsung terkoneksi dengan layanan satelit orbit rendah. Di sisi lain, keterlibatan aktif komunitas siber juga berperan dalam mempercepat proses identifikasi dini terhadap kemungkinan ancaman, sedangkan kolaborasi dengan penyedia layanan membuka peluang untuk merancang sistem keamanan siber yang lebih tanggap dan disesuaikan dengan karakteristik data lokal. Sementara itu, pemerintah memegang peran kunci dalam merumuskan kebijakan insentif dan regulasi yang mendorong transparansi informasi serta fasilitasi pertukaran pengetahuan dan praktik terbaik di antara para pemangku kepentingan (Hu 2024).

Dalam konteks Indonesia, kolaborasi antara BSSN, Kominfo, dan penyelenggara layanan lokal menjadi penting untuk mencegah dominasi teknologi luar negeri yang berpotensi memonopoli kontrol infrastruktur digital nasional.

Negara-negara seperti Thailand, India, dan Brasil menunjukkan bahwa kebijakan ketat terhadap entitas luar negeri, termasuk kewajiban pembangunan ground station domestik dan keterlibatan dalam sistem pengawasan nasional, dapat memperkuat posisi negara dalam menghadapi teknologi satelit global (Ojala dan Baber 2024). Studi komparatif menunjukkan bahwa tanpa intervensi kebijakan yang proaktif, negara-negara berkembang akan tetap menjadi pasar pasif tanpa kendali atas keamanan dan keberlanjutan digitalnya(Lin, Matthews, dan Olsen 2024).

Hasil sintesis tematik dari 18 studi yang dikaji dalam penelitian ini menunjukkan bahwa kehadiran Starlink sebagai penyedia layanan internet berbasis satelit orbit rendah (LEO) tidak dapat dilepaskan dari berbagai implikasi multidimensi terhadap keamanan jaringan nasional. Ketiga tema utama yang ditemukan kerentanan infrastruktur teknis, ketimpangan regulasi, dan ancaman terhadap kedaulatan digital secara nyata saling terkait dan mengarah pada satu kesimpulan penting: bahwa adopsi teknologi global tanpa kesiapan lokal yang setara akan menciptakan asimetri yang melemahkan posisi negara dalam menjaga kepentingan strategisnya.

Dari perspektif kerangka NIST Cybersecurity Framework, ancaman-ancaman teknis yang ditemukan dalam layanan Starlink, seperti kemungkinan serangan DoS, spoofing, dan eksploitasi terminal pengguna, menunjukkan bahwa fungsi-fungsi dasar seperti detection, response, dan recovery belum dapat diimplementasikan secara menyeluruh dalam konteks Indonesia (Smailes dkk. 2023). Hal ini terjadi karena layanan ini tidak sepenuhnya berada dalam jangkauan pengawasan infrastruktur nasional. Dalam konteks tersebut, pendekatan keamanan pasif menjadi tidak memadai. Sebaliknya, dibutuhkan sistem pertahanan aktif dan kolaboratif yang menjangkau hingga ke penyedia layanan lintas batas.

Dari sisi regulasi, analisis menunjukkan adanya ketidaksesuaian antara sistem hukum nasional dengan realitas teknologi global. Meskipun Indonesia telah memiliki peraturan yang mencakup perlindungan data pribadi dan penyelenggaraan telekomunikasi, belum tersedia perangkat hukum yang secara khusus mengatur tata kelola teknologi orbit rendah, pengawasan lalu lintas data satelit, serta pembagian tanggung jawab hukum antara pemerintah dan penyedia asing. Ketimpangan ini menunjukkan bahwa regulatory lag bukan hanya terjadi karena keterlambatan legislasi, tetapi juga karena absennya mekanisme adaptif yang mampu mengikuti perkembangan teknologi secara real-time. Sebagai contoh, tidak adanya kewajiban bagi Starlink untuk membangun network operation center atau ground control di

Indonesia menyebabkan seluruh trafik data dikendalikan dari luar negeri, menjauhkan pemerintah dari kendali operasional layanan tersebut (Satryoko dan Runturambi 2020).

Secara teoritis, temuan ini memperluas pemahaman kita mengenai konsep kedaulatan digital dalam konteks negara berkembang. Jika sebelumnya isu kedaulatan digital lebih banyak dibahas dalam kerangka data localization dan proteksi informasi, kini perluasan makna mencakup pula hak negara atas kendali fisik dan virtual terhadap penyedia layanan asing. Dalam kerangka ini, kedaulatan tidak hanya berarti mengatur, tetapi juga mencakup kemampuan teknis dan hukum untuk mengawasi serta menegakkan kepatuhan dalam konteks lintas yurisdiksi. Temuan ini sejalan dengan literatur mutakhir yang menekankan pentingnya cyber-sovereignty sebagai bagian dari keamanan nasional yang integral, bukan sekadar turunan dari kebijakan komunikasi(Pierucci 2025).

Kontribusi ilmiah dari penelitian ini dapat dilihat dari tiga sisi utama:

1. Kontribusi terhadap Literasi Akademik Keamanan Jaringan

Penelitian ini memperkuat pentingnya pendekatan sintesis tematik dalam SLR untuk mengungkap kompleksitas multidimensi dari fenomena teknologi global seperti Starlink. Tidak hanya membahas aspek teknis, hasil studi juga menunjukkan relevansi dimensi hukum, sosial, dan geopolitik dalam menentukan arah kebijakan digital suatu negara. Dengan mengintegrasikan hasil temuan ke dalam kerangka berpikir yang kontekstual, penelitian ini memperluas literatur mengenai keamanan digital berbasis infrastruktur satelit di negara berkembang.

2. Kontribusi terhadap Formulasi Kebijakan Nasional

Bagi pembuat kebijakan di Indonesia, hasil ini memberikan basis argumentasi untuk mendesak pembentukan regulasi spesifik terkait operasional layanan satelit orbit rendah. Temuan-temuan ini merekomendasikan adanya penyesuaian kebijakan yang mencakup: (1) kewajiban interconnection point di dalam negeri, (2) audit sistem keamanan dan lalu lintas data, serta (3) kerjasama antara pemerintah dan operator dalam membangun protokol perlindungan infrastruktur vital. Penelitian ini juga menunjukkan bahwa keterlibatan multi-aktor sangat penting, mencakup lembaga seperti BSSN, Kominfo, sektor swasta, serta komunitas siber.

3. Kontribusi terhadap Wacana Kedaulatan Digital di Negara Berkembang

Secara konseptual, studi ini menempatkan isu Starlink tidak hanya sebagai persoalan teknologi, tetapi sebagai arena kontestasi kedaulatan digital. Dalam konteks negara berkembang seperti Indonesia, yang memiliki keterbatasan dalam hal teknologi pengawasan dan kekuatan regulatif, kedaulatan digital hanya dapat dicapai jika diiringi oleh kemauan politik yang kuat dan investasi dalam infrastruktur strategis. Dengan menunjukkan bagaimana ketidakseimbangan kekuasaan digital dapat mengarah pada ketergantungan struktural terhadap teknologi asing, penelitian ini menyumbangkan perspektif baru dalam debat internasional mengenai keadilan teknologi.

Studi ini memberikan pembelajaran penting mengenai bagaimana pendekatan akademik berbasis sistematik dan tematik dapat mendukung reformasi kebijakan berbasis bukti. Dengan memanfaatkan model SLR berbasis PRISMA yang dikombinasikan dengan sintesis tematik mendalam, penelitian ini menghadirkan metodologi yang dapat direplikasi dalam isu-isu strategis lain yang berkaitan dengan teknologi transnasional.

5. KESIMPULAN

Penelitian ini menyimpulkan bahwa kehadiran Starlink sebagai penyedia layanan internet berbasis satelit orbit rendah membawa konsekuensi strategis terhadap keamanan jaringan nasional Indonesia. Dengan mengadopsi pendekatan Systematic Literature Review (SLR) berbasis PRISMA 2020 dan sintesis tematik, studi ini menemukan tiga isu utama: kerentanan teknis infrastruktur satelit terhadap serangan siber, ketidaksiapan regulasi nasional dalam mengatur entitas asing, serta lemahnya pengendalian negara atas aliran dan penyimpanan data lintas batas.

Starlink beroperasi di luar jaringan nasional, sehingga mekanisme pengawasan pemerintah menjadi terbatas. Hal ini berimplikasi serius terhadap fungsi deteksi, proteksi, dan respons keamanan yang disusun dalam kerangka NIST Cybersecurity Framework. Tanpa keterlibatan negara dalam pengelolaan gateway, arsitektur, dan audit lalu lintas data, Indonesia kehilangan sebagian kendali atas ruang digitalnya. Dalam konteks ini, kedaulatan digital bukan hanya soal penyimpanan data, tetapi juga kontrol menyeluruh atas struktur jaringan, perizinan, dan protokol keamanan.

Kontribusi penelitian ini tidak hanya memperkuat literatur akademik mengenai ancaman teknologi global, tetapi juga memberikan masukan langsung bagi pembuat kebijakan nasional. Pemerintah perlu segera membangun regulasi spesifik yang mengatur layanan satelit asing—termasuk syarat interkoneksi domestik dan audit keamanan. Selain itu, perlu dikembangkan standar nasional keamanan digital untuk mencegah dominasi penyedia global yang tidak setara dengan penyedia lokal dalam hal tanggung jawab hukum dan teknis.

Dengan demikian, meskipun Starlink menawarkan solusi untuk kesenjangan konektivitas, jika tidak diimbangi dengan penguatan struktur regulatif dan teknis dalam negeri, maka ketergantungan terhadap layanan asing akan melemahkan posisi strategis negara dalam menjaga keamanan dan kedaulatan di era digital. Indonesia harus segera bergerak dari sekadar menjadi pengguna teknologi menjadi negara yang mampu mengatur dan melindungi ruang digitalnya secara utuh dan berdaulat.

Daftar Pustaka

Bakyt, Makhabbat, Luigi La Spada, Nida Zeeshan, Khuralay Moldamurat, Sabyrzhan Atanov, Assem Konyrkhanova, Nikolay Yurkov, Absalyam Kuanysh, Yertis Marat, dan Alzhan Tilenbayev. 2025. "Advanced Cybersecurity Framework for LEO Aerospace: Integrating Quantum Cryptography, Artificial Intelligence Anomaly Detection, and Blockchain Technology." *Journal of Robotics and Control (JRC)* 6(2):695–714. doi:10.18196/jrc.v6i2.25918.

Boeira, Demétrio F., Eder J. Scheid, Muriel F. Franco, Luciano Zembruzki, dan Lisandro Z. Granville. 2023. "Traffic Centralization and Digital Sovereignty: An Analysis Under the Lens of DNS Servers." doi:10.1109/noms59830.2024.10575700.

Coche, Eugénie, Ans Kolk, dan Václav Ocelík. 2024. "Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business." *Journal of International Business Policy* 7(1):112–27.

Credi, Ottavia, dan Camilla Vianini. 2021. "Space and European Digital Sovereignty." https://www.newspace.im/constellations/hongyun.

Darmayadi, Andrias, Fatma Sania Aprilia, Yasmin Khairunisa Somantri, Fikri Andriansyah Pamungkas, Anisa Nurfadhilah, dan Sri Wahyuni Sinambela. 2025. "Strategy and Implementation of Indonesian Cyber Diplomacy in the Framework of Bilateral and Multilateral Cooperation in the Digital Era." Hlm. 105–19 dalam.

Dinis, J. ,. et al. 2022. "Cybersecurity Collaboration in National Defense Satellite Networks." *Defence and Peace Economics*.

Garcia-Cabeza, Jorge, Javier Albert-Smet, Zoraida Frias, Luis Mendo, Santiago Andrés Azcoitia, dan Eduardo Yraola. 2025. "Direct-to-Cell: A First Look into Starlink's Direct Satellite-to-Device Radio Access Network through Crowdsourced Measurements." http://arxiv.org/abs/2506.00283.

Ghozie Afiansyah, Hafizh, Nur Annisa, dan Kadarwati Febriyani. 2023. *Penyusunan Kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST CSF 2.0 dan ISO/IEC 27001:2022*.

Hukunala, Sandy Victor. 2024. "STARLINK ON COMPETITION OF INTERNET PROVIDERS IN INDONESIA: A BUSINESS LAW REVIEW." *Authentica* 7(1):1–9. doi:10.20884/1.atc.2024.7.1.455.

Hu, Peng. 2024. "Closing the Performance and Management Gaps with Satellite Internet: Challenges, Approaches, and Future Directions." http://arxiv.org/abs/2401.07842.

Indirwan, dan Sarah Safira Aulianisa. 2020. "Critical Review of The Urgency of Strenghthening The Implementation of Cyber Security and Resilience in Indonesia." *Lex Scientia Law Review* 4(1):30–45. doi:10.15294/lesrev.v4i1.38197.

Irawan Hafizhan, Muhammad Alva Hendi, dan Nasiri Asro. 2024. "Design of Cybersecurity Maturity Assessment Framework Using NIST CSF v1.1 and CIS Controls v8." *JURNAL INOVTEK POLBENG - SERI INFORMATIKA* 9 (1_.

Kareem, Karwan Mustafa. t.t. *Cyber Threat Landscape Analysis for Starlink Assessing Risks and Mitigation Strategies in the Global Satellite Internet Infrastructure*.

Kassem, H. ,. Niyato, D. ,. &. Kim, D. I. 2022. "Throughput Optimization in Satellite Internet Systems." *Wireless Networks*.

Khaliq, Moh Yusuf, Muhammad Rakib, dan Valentino Aris. 2024. *Sentiment Analysis to Starlink Services in Indonesia*. www.ijltem.com.

Kwentoa, Ifeanyi Kingsley. 2025. "Cybersecurity in Digital Sovereignty: Protecting National Digital Ecosystems against Foreign Cyber Infiltration in the Age of Decentralized Technology." 1(4). www.jngr5.com.

Lin, Kun Chin, William Matthews, dan Sam Olsen. 2024. "Middle spacepowers' integration with the global supply chain for the space industry: Taiwan and Thailand." *Business and Politics*. doi:10.1017/bap.2024.18.

Ma, Sami, Yi Ching Chou, Miao Zhang, Hao Fang, Haoyuan Zhao, Jiangchuan Liu, dan William I. Atlas. 2024. "LEO Satellite Network Access in the Wild: Potentials, Experiences, and Challenges." *IEEE Network* 38(6):396–403. doi:10.1109/MNET.2024.3391271.

Michel, F. et al. 2022. "A First Look at Starlink Performance." *Proceedings of the 22nd ACM Internet Measurement Conference*. doi:https://doi.org/10.1145/3517745.3561457.

Monash Hub. 2024. "Digital Health and Starlink in Indonesia." *Monash University Indonesia Discussion Paper Series*.

Nudan, Pankrasius Wahu, Pujo Widodo, dan M. Affifudin. 2024. "Navigating the Starlink Era of Personal Data Protection in Indonesia." *Formosa Journal of Science and Technology* 3(7):1447–58. doi:10.55927/fjst.v3i7.10139.

Ogutu, Osoro B., dan Edward J. Oughton. 2021. "A Techno-Economic Cost Framework for Satellite Networks Applied to Low Earth Orbit Constellations: Assessing Starlink, OneWeb and Kuiper." http://arxiv.org/abs/2108.10834.

Ojala, Arto, dan William W. Baber. 2024. *Space Business: Emerging Theory and Practice*. Springer Nature.

Ortiz, Flor, Eva Lagunas, Almoatssimbillah Saifaldawla, Mahdis Jalali, Luis Emiliani, dan Symeon Chatzinotas. 2024. "Emerging NGSO Constellations: Spectral Coexistence with GSO Satellite Communication Systems." http://arxiv.org/abs/2404.12651.

Pan, J. ,. Zhao, J. ,. &. Cai, L. 2023. "Measuring a Low-Earth-Orbit Satellite Network." *IEEE Communications Magazine*. doi:https://doi.org/10.1007/s11235-022-00987-2.

Peled, Roy, Eran Aizikovich, Edan Habler, Yuval Elovici, dan Asaf Shabtai. 2023. "Evaluating the Security of Satellite Systems." http://arxiv.org/abs/2312.01330.

Pierucci, Federico. 2025. "Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace." *Digital Society* 4(1). doi:10.1007/s44206-025-00189-4.

Priyanka, E. B. et al. 2021. "Advanced Cybersecurity Framework for LEO Aerospace." *Journal of Robotics and Control*. doi:https://doi.org/10.18196/jrc.v2i6.12145.

Putro, Y. M. et al. 2023. "Satellite Mega Constellations and National Sovereignty." *Brawijaya Law Journal*. doi:https://doi.org/10.21776/ub.blj.2023.010.01.06.

Roberts, Huw. 2024. "Digital sovereignty and artificial intelligence: a normative approach." *Ethics and Information Technology* 26(4). doi:10.1007/s10676-024-09810-5.

Satryoko, A., dan Runturambi. 2020. "Strategi Indonesia Menghadapi Era Konstalasi Low Earth Orbit Satelit Dalam Kemungkinan Penggunannya Oleh Intelijen Asing Sebagai Alat Spionase." *Jurnal Kajian Stratejik Ketahanan Nasional* 3(1). doi:10.7454/jkskn.v3i1.10033.

Shaengchart, Yarnaphat, dan Tanpat Kraiwanit. 2024. "THE SPACEX STARLINK SATELLITE PROJECT: BUSINESS STRATEGIES AND PERSPECTIVES." *Corporate and Business Strategy Review* 5(1):30–37. doi:10.22495/cbsrv5i1art3.

Shukur, Hazrul Hafiz Abdul, Yasser Asrul Ahmad, Muhammad Sharir Fathullah Mohd Yunus, dan Khairayu Badron. 2025. "LATENCY PERFORMANCE EVALUATION OF LEO STARLINK AND SES-12 GEO HTS NETWORK UNDER TROPICAL RAINFALL CONDITIONS." *IIUM Engineering Journal* 26(2):204–19. doi:10.31436/iiumej.v26i2.3653.

Sitouah, Nacereddine, Fatiha Merazka, dan Abdenour Hedjazi. 2022. "Deep learning approach for interruption attacks detection in LEO satellite networks." http://arxiv.org/abs/2301.03998.

Smailes, Joshua, Edd Salkield, Sebastian Köhler, Simon Birnbach, dan Ivan Martinovic. 2023. "Dishing Out DoS: How to Disable and Secure the Starlink User Terminal." http://arxiv.org/abs/2303.00582.

Tanjung, Dio Febrilian, Oky Dwi Nurhayati, dan Adi Wibowo. 2024. "Design Information Security in Electronic-Based Government Systems Using NIST CSF 2.0, ISO/IEC 27001: 2022 and CIS Control." *International Journal of Innovative Science and Research Technology (IJISRT)* 523–30. doi:10.38124/ijisrt/ijisrt24jun1212.

Tedeschi, Pietro, Savio Sciancalepore, dan Roberto Di Pietro. 2022. "Satellite-Based Communications Security: A Survey of Threats, Solutions, and Research Challenges." doi:10.1016/j.comnet.2022.109246.

Westphal, Cedric, Lin Han, dan Richard Li. 2023. "LEO Satellite Networking Relaunched: Survey and Current Research Challenges." http://arxiv.org/abs/2310.07646.

Yue, Pingyue, Jianping An, Jiankang Zhang, Jia Ye, Gaofeng Pan, Shuai Wang, Pei Xiao, dan Lajos Hanzo. 2022. "Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead." http://arxiv.org/abs/2201.03063.

Zhang, Chaoyu, Hexuan Yu, Shanghao Shi, Shaoyu Li, Yi Shi, Eric Burger, Y. Thomas Hou, dan Wenjing Lou. 2025. "StarCast: A Secure and Spectrum-Efficient Group Communication Scheme for LEO Satellite Networks." http://arxiv.org/abs/2502.07901.