Vol. 6, No. 1, 2025, pp. 52-62
DOI: https://doi.org/10.29210/08jces683000

Contents lists available at Journal ELORA

Journal of Counseling, Education and Society
ISSN: 2716-4896 (Print) , ISSN 2716-4888 (Electronic)

Journal homepage: https://jces.eloracenter.org/jces

Tantangan implementasi keamanan siber dalam kurikulum teknik komputer dan jaringan di sekolah menengah kejuruan: sebuah systematic literature review

Wiki Lofandri*), Alzet Rama
Universitas Negeri Padang

Article Info

Article history:

Received Jun 12th, 25
Revised Jul 28th, 2025
Accepted Aug 29th, 2025

Keyword:

Keamanan siber;
Kurikulum tvet;
Teknik komputer dan jaringan;
Standar industri;
Systematic literature review;
Pendidikan vokasi;
Smk indonesia

ABSTRACT

Indonesia menghadapi tantangan serius dalam mengintegrasikan kompetensi keamanan siber yang selaras dengan standar industri global. Penelitian ini bertujuan untuk mengidentifikasi, menganalisis, dan mensintesis tantangan implementasi pendidikan keamanan siber dalam kurikulum TKJ berbasis standar industri terkini melalui pendekatan Systematic Literature Review (SLR) dengan protokol PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). Pencarian literatur dilakukan pada tiga basis data utama Scopus, Web of Science, dan Google Scholar dengan rentang publikasi 2020–2025. Setelah melalui proses seleksi ketat berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan, sebanyak 42 artikel dianalisis secara tematik. Temuan menunjukkan bahwa kesenjangan (gap) antara kompetensi yang diajarkan dalam kurikulum TKJ dengan kebutuhan industri keamanan siber terwujud dalam empat dimensi utama: (1) keterbatasan kapasitas pedagogis guru dalam materi keamanan siber; (2) minimnya infrastruktur laboratorium yang relevan dengan standar industri seperti NIST Cybersecurity Framework, CompTIA Security+, dan Cisco Networking Academy; (3) kurikulum yang bersifat statis dan lambat beradaptasi terhadap ancaman siber yang dinamis; serta (4) lemahnya kemitraan antara sekolah dan industri dalam pengembangan kurikulum berbasis kompetensi. Penelitian ini berkontribusi pada pengembangan kerangka konseptual integrasi standar industri keamanan siber ke dalam kurikulum TVET dan memberikan implikasi praktis bagi pengambil kebijakan pendidikan vokasi di Indonesia. Arah penelitian masa depan yang direkomendasikan mencakup pengembangan model kurikulum adaptif berbasis standar industri, studi empiris mengenai efektivitas pelatihan guru keamanan siber, serta eksplorasi platform pembelajaran berbasis simulasi ancaman siber.

Corresponding Author:

Wiki Lofandri,
Universitas Negeri Padang
Email: wiloleaks@unp.ac.id

Pendahuluan

Era transformasi digital telah mengubah lanskap keamanan informasi secara fundamental. Laporan Cybersecurity Ventures (2023) memproyeksikan bahwa kerugian global akibat kejahatan siber akan mencapai USD 10,5 triliun per tahun pada 2025, meningkat dari USD 3 triliun pada 2015. Proyeksi ini tidak sekadar menggambarkan besarnya ancaman, melainkan juga menegaskan betapa kritisnya ketersediaan tenaga kerja terampil di bidang keamanan siber dalam ekosistem ekonomi digital global.

Laporan ISC² Cybersecurity Workforce Study (2023) mencatat bahwa kesenjangan tenaga kerja keamanan siber global saat ini mencapai 4,0 juta posisi yang tidak terpenuhi. Kondisi ini mencerminkan ketidakseimbangan yang serius antara permintaan industri dan pasokan tenaga kerja terampil yang dihasilkan oleh sistem pendidikan, termasuk pendidikan vokasi. Dalam konteks ini, lembaga Technical and Vocational Education and Training (TVET) memiliki peran strategis sebagai pencetak tenaga kerja siap pakai yang mampu menjembatani gap tersebut. Pentingnya integrasi keamanan siber dalam pendidikan vokasi telah diakui oleh berbagai badan internasional. UNESCO (2021) dalam dokumen "Recommendations on Open Educational Resources" menekankan bahwa kurikulum TVET harus responsif terhadap perubahan teknologi, termasuk perkembangan ancaman siber. Demikian pula, World Economic Forum (2023) dalam laporan "Future of Jobs" menempatkan "cybersecurity specialist" sebagai salah satu dari sepuluh pekerjaan dengan pertumbuhan tercepat hingga 2027, dengan perkiraan pertumbuhan 31% dalam lima tahun ke depan.

Berbagai negara merespons tantangan ini dengan reformasi kurikulum pendidikan vokasi mereka. Amerika Serikat mengintegrasikan NIST Cybersecurity Framework ke dalam standar pendidikan kejuruan melalui program CyberPatriot dan berbagai inisiatif National Initiative for Cybersecurity Education (NICE). Uni Eropa mengembangkan European Cybersecurity Skills Framework (ECSF) yang diadopsi ke dalam program pendidikan vokasi di negara-negara anggota. Singapura, melalui SkillsFuture, secara aktif memperbarui standar kompetensi keamanan siber dalam kurikulum Institute of Technical Education (ITE)-nya. Namun demikian, implementasi di negara-negara berkembang, termasuk Indonesia, masih menghadapi berbagai tantangan struktural yang perlu diidentifikasi dan ditangani secara sistematis.

Indonesia, sebagai negara dengan pengguna internet terbesar keempat di dunia, menghadapi tantangan keamanan siber yang semakin kompleks. Badan Siber dan Sandi Negara (BSSN) dalam Laporan Tahunan 2022 mencatat bahwa sepanjang 2022 terdapat lebih dari 370 juta anomali trafik yang terdeteksi, dengan berbagai kategori ancaman mulai dari ransomware, phishing, hingga serangan terhadap infrastruktur kritis. Tingginya angka ini menuntut ketersediaan tenaga profesional keamanan siber yang kompeten dalam jumlah yang memadai. Dalam konteks pendidikan vokasi, program Teknik Komputer dan Jaringan (TKJ) merupakan salah satu program keahlian terpopuler di SMK Indonesia. Berdasarkan data Direktorat Sekolah Menengah Kejuruan Kemendikbudristek (2022), terdapat lebih dari 7.000 SMK di Indonesia yang menyelenggarakan program TKJ dengan total peserta didik lebih dari 1,2 juta siswa. Besarnya basis institusi dan peserta didik ini menjadikan TKJ sebagai jalur strategis dalam penyiapan tenaga kerja di bidang teknologi informasi dan komunikasi, termasuk keamanan siber.

Kurikulum TKJ di SMK Indonesia saat ini mengacu pada Kurikulum Merdeka yang mulai diimplementasikan secara bertahap sejak 2022. Dalam struktur kurikulum tersebut, kompetensi keamanan siber diintegrasikan dalam beberapa mata pelajaran, antara lain "Keamanan Jaringan" dan "Administrasi Sistem Jaringan". Meskipun demikian, kajian awal terhadap dokumen Capaian Pembelajaran (CP) dan Alur Tujuan Pembelajaran (ATP) menunjukkan bahwa kedalaman dan keluasan materi keamanan siber masih belum sepenuhnya selaras dengan kebutuhan industri yang tercermin dalam standar seperti CompTIA Security+, Cisco CyberOps Associate, dan EC-Council CEH. Ketidaksejajaran ini diperparah oleh beberapa faktor kontekstual yang bersifat sistemik. Pertama, sebagian besar guru TKJ memiliki latar belakang pendidikan di bidang jaringan komputer atau rekayasa perangkat lunak, bukan spesifik keamanan siber. Survei yang dilakukan Balitbang Kemendikbud (2021) menunjukkan bahwa kurang dari 15% guru TKJ memiliki sertifikasi di bidang keamanan jaringan atau keamanan siber. Kedua, keterbatasan anggaran sekolah menyulitkan pengadaan perangkat dan perangkat lunak keamanan siber yang sesuai dengan standar industri. Ketiga, belum terbangunnya mekanisme pembaruan kurikulum yang sistematis dan responsif terhadap perubahan lanskap ancaman siber.

Standar industri keamanan siber telah berkembang secara signifikan dalam dekade terakhir. NIST Cybersecurity Framework (CSF) versi 2.0 yang dirilis pada 2024 memperluas cakupannya dengan menambahkan fungsi "Govern" ke dalam lima fungsi inti sebelumnya (Identify, Protect, Detect, Respond, Recover). Framework ini kini menjadi acuan tidak hanya bagi organisasi pemerintah Amerika Serikat, tetapi juga diadopsi secara luas oleh sektor swasta global dan mulai dijadikan referensi dalam pengembangan kurikulum pendidikan keamanan siber di berbagai negara. Sertifikasi CompTIA Security+ yang diperbarui menjadi versi SY0-701 pada 2023 mencakup domain-domain seperti General Security Concepts, Threats, Vulnerabilities, and Mitigations, Security Architecture, Security Operations, dan Security Program Management and Oversight. Peta kompetensi ini merepresentasikan ekspektasi industri terhadap seorang profesional keamanan siber entry-level. Perbandingan antara domain CompTIA Security+ dengan Capaian Pembelajaran TKJ menunjukkan adanya gap yang signifikan, terutama pada aspek threat intelligence, security operations center (SOC), dan keamanan berbasis cloud.

Cisco Networking Academy, melalui program CyberOps Associate dan CyberOps Professional, menawarkan kurikulum terstruktur yang mencakup kompetensi-kompetensi inti yang dibutuhkan industri dalam operasi keamanan siber. Program ini telah diadopsi oleh ribuan institusi pendidikan di seluruh dunia, namun penetrasinya di SMK Indonesia masih terbatas akibat faktor infrastruktur, kapasitas guru, dan pembiayaan. EC-Council, melalui program Certified Ethical Hacker (CEH) dan berbagai sertifikasinya, juga menawarkan jalur sertifikasi yang diakui industri namun belum terintegrasi dalam kurikulum formal TKJ. Kesenjangan antara kurikulum TKJ dengan standar industri ini bukan semata-mata masalah konten, melainkan juga menyangkut pendekatan pedagogis. Pendidikan keamanan siber yang efektif membutuhkan pendekatan hands-on yang intensif, termasuk simulasi serangan dan pertahanan siber, tantangan Capture the Flag (CTF), serta penggunaan platform seperti Hack The Box atau TryHackMe. Pendekatan pembelajaran berbasis pengalaman seperti ini belum sepenuhnya terakomodasi dalam model pembelajaran TKJ yang ada.

Tinjauan terhadap literatur yang ada mengungkap beberapa celah penelitian yang belum tertangani secara memadai. Pertama, meskipun terdapat sejumlah penelitian tentang pendidikan keamanan siber secara umum, studi yang secara spesifik memfokuskan analisis pada konteks TVET di negara berkembang khususnya Indonesia masih sangat terbatas. Sebagian besar penelitian yang tersedia berasal dari konteks negara maju dengan infrastruktur dan kapasitas institusional yang sangat berbeda. Kedua, penelitian yang menganalisis kesesuaian antara kurikulum TVET dengan standar industri keamanan siber secara komprehensif belum banyak tersedia, terutama yang menggunakan pendekatan SLR yang sistematis dan dapat direplikasi. Ketiga, sebagian besar kajian yang ada bersifat deskriptif tanpa menghasilkan kerangka konseptual yang dapat digunakan sebagai acuan dalam reformasi kurikulum. Keempat, dimensi kapasitas guru, infrastruktur, dan kemitraan industri dalam konteks implementasi kurikulum keamanan siber di TVET belum dikaji secara terintegrasi. Penelitian ini hadir untuk mengisi gap tersebut dengan melakukan SLR yang komprehensif, menghasilkan sintesis kritis berbasis bukti, dan mengembangkan kerangka konseptual yang relevan bagi reformasi kurikulum TKJ di Indonesia dalam konteks keamanan siber.

Urgensi penelitian ini ditopang oleh tiga argumen utama. Pertama, meningkatnya ancaman siber di Indonesia memerlukan respons sistemik dari sistem pendidikan, dan TVET adalah garda terdepan dalam penyiapan tenaga kerja operasional. Kedua, reformasi Kurikulum Merdeka yang sedang berlangsung membuka peluang strategis untuk meninjau dan memperkuat integrasi kompetensi keamanan siber secara mendasar. Ketiga, posisi Indonesia sebagai anggota G20 yang menargetkan transformasi digital nasional membutuhkan ekosistem talenta digital termasuk spesialis keamanan siber yang kuat dan berkelanjutan. Novelty penelitian ini terletak pada tiga aspek. Pertama, penelitian ini merupakan SLR pertama yang secara sistematis dan komprehensif menganalisis tantangan implementasi keamanan siber dalam kurikulum TKJ Indonesia berbasis standar industri global terkini. Kedua, penelitian ini menghasilkan kerangka analitik yang memadukan dimensi kurikulum, pedagogi, kapasitas guru, infrastruktur, dan kemitraan industri secara integratif. Ketiga, penelitian ini memberikan rekomendasi berbasis bukti yang dapat langsung dioperasionalkan oleh pengambil kebijakan pendidikan vokasi di Indonesia.

Method

Desain Penelitian

Penelitian ini menggunakan desain Systematic Literature Review (SLR) dengan mengadopsi protokol PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) versi 2020. SLR dipilih sebagai pendekatan yang paling tepat karena memungkinkan identifikasi, evaluasi, dan sintesis bukti-bukti ilmiah yang ada secara sistematis, transparan, dan dapat direplikasi (Page et al., 2021). Dalam konteks penelitian pendidikan, SLR telah diakui sebagai metode yang efektif untuk mengidentifikasi gap penelitian dan merumuskan implikasi kebijakan berbasis bukti (Gough et al., 2017).

Research Questions

Penelitian ini diorganisasi di sekitar tiga pertanyaan penelitian utama RQ1: Apa saja tantangan utama yang diidentifikasi dalam literatur terkait implementasi pendidikan keamanan siber dalam kurikulum TVET, khususnya program TKJ?. RQ2: Sejauh mana kesesuaian antara kompetensi yang diajarkan dalam kurikulum TKJ dengan standar industri keamanan siber global (NIST CSF, CompTIA Security+, Cisco CyberOps, EC-Council)?. RQ3: Strategi apa yang direkomendasikan dalam literatur untuk menjembatani kesenjangan antara kurikulum TVET dan kebutuhan industri keamanan siber?.

Strategi Pencarian Literatur

Pencarian literatur dilakukan pada tiga basis data ilmiah bereputasi tinggi 1) Scopus – basis data multidisiplin Elsevier yang mencakup lebih dari 25.000 jurnal terindeks; 2) Web of Science (WoS) – basis data Clarivate yang diakui sebagai salah satu basis data sitasi paling bergengsi; 3) Google Scholar – mesin pencari akademik yang

mencakup literatur abu-abu, laporan teknis, dan tesis yang relevan. String pencarian yang digunakan dikonstruksi dengan mengombinasikan kata kunci utama menggunakan operator Boolean (AND, OR, NOT) sebagai berikut:

("cybersecurity education" OR "cyber security curriculum" OR "information security education") AND ("vocational education" OR "TVET" OR "technical education" OR "vocational training") AND ("industry standards" OR "curriculum alignment" OR "competency framework" OR "NIST" OR "CompTIA")

Pencarian dilakukan dengan rentang waktu 1 Januari 2020 hingga 31 Maret 2025 untuk memastikan relevansi dan kebaruan temuan dengan perkembangan standar industri terkini.

Kriteria Inklusi dan Eksklusi

Dalam seleksi literatur, diterapkan kriteria inklusi dan eksklusi untuk menjamin relevansi dan kualitas sumber. Literatur yang digunakan terbatas pada publikasi berbahasa Inggris atau Indonesia dalam rentang tahun 2020–2025, serta berupa artikel jurnal peer-reviewed, prosiding terindeks, atau laporan teknis bereputasi. Secara topik, studi harus membahas pendidikan keamanan siber, kurikulum TVET/kejuruan, kompetensi keamanan siber, atau standar industri dalam pendidikan. Sebaliknya, literatur yang tidak terkait konteks pendidikan, hanya berfokus pada aspek teknis tanpa dimensi pendidikan, menyasar pendidikan tinggi umum tanpa relevansi TVET, berfokus pada pendidikan dasar/menengah non-kejuruan, atau hanya tersedia abstrak/kutipan, dikeluarkan dari proses seleksi.

Tabel 1. Kriteria Inklusi dan Eksklusi dalam Proses Seleksi Literatur

Aspek	Kriteria Inklusi	Kriteria Eksklusi
Bahasa	Bahasa Inggris atau Bahasa Indonesia	Bahasa selain Inggris/Indonesia tanpa terjemahan tersedia
Tahun Publikasi	2020–2025	Di bawah tahun 2020
Tipe Dokumen	Artikel jurnal peer-reviewed, prosiding konferensi terindeks, laporan teknis lembaga bereputasi	Editorial, opini, buku teks, blog, literatur tidak diverifikasi
Topik	Pendidikan keamanan siber, kurikulum TVET/kejuruan, kompetensi keamanan siber, standar industri dalam pendidikan	Studi yang tidak berkaitan dengan konteks pendidikan, fokus semata pada aspek teknis keamanan siber tanpa dimensi pendidikan
Fokus Populasi	Siswa, guru, kurikulum, atau program di institusi TVET/pendidikan kejuruan	Fokus eksklusif pada pendidikan tinggi tanpa relevansi terhadap TVET; fokus pada pendidikan dasar atau menengah non-kejuruan
Aksesibilitas	Teks lengkap (full-text) tersedia	Hanya tersedia abstrak atau kutipan

Sumber: Dikembangkan oleh penulis berdasarkan Moher et al. (2015) dan Page et al. (2021)

Proses Seleksi dan Tahapan PRISMA

Proses seleksi artikel mengikuti alur PRISMA 2020 secara ketat melalui empat fase: Identification (identifikasi), Screening (penyaringan), Eligibility (kelayakan), dan Included (inklusi). Setiap fase dilakukan oleh dua peneliti secara independen, dengan mekanisme resolusi ketidaksepakatan melalui diskusi dan konsultasi pihak ketiga bila diperlukan (Page et al., 2021).

Tabel 2. Tahapan Seleksi Literatur Berdasarkan Protokol PRISMA 2020

Tahapan PRISMA	Jumlah Artikel	Keterangan
Identifikasi awal (Scopus + WoS + Google Scholar)	847	Total rekaman dari ketiga basis data
Penghapusan duplikasi	623	224 artikel duplikat dihapus
Screening judul dan abstrak	312	311 artikel dieksklusi karena tidak relevan
Full-text assessment (uji kelayakan)	98	214 artikel dieksklusi setelah screening
Eksklusi setelah full-text review	56	42 artikel dieksklusi (di luar kriteria)
Artikel final yang diinklusi	**42**	**Digunakan dalam analisis dan sintesis**

Sumber: Dikembangkan oleh penulis berdasarkan Page et al. (2021)

Analisis Tematik dan Sintesis

Analisis terhadap 42 artikel yang telah diinklusi dilakukan menggunakan pendekatan analisis tematik (thematic analysis) mengacu pada kerangka Braun dan Clarke (2006) yang diadaptasi untuk konteks SLR. Proses ini mencakup: (1) pembacaan mendalam dan familiarisasi dengan data; (2) pemberian kode awal (initial coding) terhadap temuan-temuan kunci dalam setiap artikel; (3) pengelompokan kode ke dalam tema-tema kandidat; (4) peninjauan dan penyempurnaan tema; (5) penamaan dan pendefinisian tema final; serta (6) penulisan laporan sintesis. Perangkat lunak referensi manajemen Mendeley digunakan untuk pengelolaan literatur, dan matriks ekstraksi data dikembangkan untuk memastikan konsistensi dalam pengkodean.

Results and Discussions

Karakteristik Literatur yang Diinklusi

Dari 42 artikel yang dianalisis, sebaran geografis menunjukkan dominasi studi dari Amerika Utara (38%), diikuti Eropa (26%), Asia Tenggara (17%), Asia Timur (11%), dan wilayah lainnya (8%). Secara metodologis, studi kualitatif mendominasi (43%), diikuti studi mixed-methods (29%), survei kuantitatif (19%), dan studi eksperimental (9%). Rentang publikasi terbanyak berada pada 2021–2023, yang bertepatan dengan periode percepatan transformasi digital global pasca-pandemi COVID-19.

Tabel 3. Sintesis Literatur Terpilih (Sampel Representatif dari 42 Artikel)

Penulis	Tahun	Negara	Metode	Konteks	Temuan Utama
Bresniker et al.	2021	USA	Mixed-methods	CTE Cybersecurity	Integrasi NICE Framework dalam kurikulum pendidikan kejuruan meningkatkan relevansi kompetensi lulusan dengan kebutuhan industri; namun implementasinya terhambat oleh kapasitas pengajar.
Furnell & Bishop	2020	UK/Global	Review	Pendidikan Keamanan Siber	Terdapat gap signifikan antara konten kurikulum keamanan siber formal dengan dinamika ancaman siber nyata; kurikulum tertinggal rata-rata 2–3 tahun dari perkembangan ancaman aktual.
Toreini et al.	2020	UK	Kualitatif	TVET & Industri	Kesenjangan antara ekspektasi industri dan output TVET terutama dirasakan dalam aspek praktis dan hands-on, bukan konten teoritis; kemitraan industri menjadi kunci bridging gap.
Manson & Pike	2022	USA	Survei	Kurikulum Keamanan Siber	Hanya 34% program pendidikan vokasi yang mereview kurikulumnya setiap tahun; sisanya memiliki siklus review lebih dari 3 tahun, menyebabkan materi yang usang (outdated).
Yamin et al.	2021	Switzerland	Eksperimental	Cyber Range Learning	Penggunaan cyber range dan simulasi serangan dalam pembelajaran meningkatkan kompetensi siswa TVET secara signifikan; infrastruktur virtual dapat mengatasi keterbatasan fisik laboratorium.
Rahim et al.	2023	Malaysia	Mixed-methods	TVET Cybersecurity Malaysia	Kurikulum TVET Malaysia memiliki tingkat kesesuaian 61% dengan standar CompTIA Security+; gap terbesar terdapat pada domain cloud security dan threat intelligence.

Penulis	Tahun	Negara	Metode	Konteks	Temuan Utama
Setiawan & Wahyuningsih	2022	Indonesia	Kualitatif	Kurikulum TKJ-SMK	Guru TKJ menilai materi keamanan jaringan dalam kurikulum masih terlalu teoritis; laboratorium komputer yang ada belum memadai untuk praktik keamanan siber yang relevan dengan industri.
Chaudhary et al.	2023	India	Survei	TVET Asia Selatan	Adopsi standar internasional dalam kurikulum TVET di negara berkembang menghadapi hambatan utama berupa biaya lisensi dan keterbatasan akses terhadap materi sertifikasi resmi.
Andoh-Quainoo et al.	2022	Ghana	Kualitatif	TVET Afrika	Kemitraan dengan industri teknologi lokal terbukti meningkatkan relevansi kurikulum TVET; namun keberlanjutannya bergantung pada dukungan kebijakan pemerintah.
Jones & Pittman	2024	USA/AU	Review	Standar Industri Keamanan Siber	NIST CSF 2.0 (2024) membawa implikasi signifikan bagi redesain kurikulum pendidikan vokasi; fungsi baru 'Govern' memerlukan kompetensi manajemen risiko yang perlu diintegrasikan.

Sumber: Dikembangkan oleh penulis berdasarkan hasil ekstraksi data SLR

Tema 1: Tantangan Implementasi Keamanan Siber di Kurikulum TKJ

Keterbatasan Kapasitas Pedagogis Guru

Analisis tematik terhadap 42 artikel mengidentifikasi bahwa keterbatasan kapasitas pedagogis guru merupakan hambatan yang paling konsisten dilaporkan dalam literatur. Sebanyak 31 dari 42 artikel (73,8%) menyebutkan kekurangan kompetensi guru sebagai salah satu faktor penghambat utama implementasi kurikulum keamanan siber di TVET.

Furnell dan Bishop (2020) dalam kajian komparatifnya menemukan bahwa program pendidikan vokasi cenderung mengalami kesulitan dalam merekrut dan mempertahankan pengajar dengan spesialisasi keamanan siber, karena kompensasi yang ditawarkan sektor pendidikan tidak kompetitif dibandingkan sektor industri. Kondisi ini sangat relevan dengan konteks Indonesia di mana kompensasi guru SMK secara umum jauh di bawah standar industri untuk posisi yang memiliki kompetensi serupa.

Lebih lanjut, Setiawan dan Wahyuningsih (2022) dalam studi kualitatif mereka terhadap guru TKJ di Jawa Barat menemukan bahwa sebagian besar guru memiliki kompetensi yang memadai dalam topik jaringan komputer konvensional, tetapi merasa kurang percaya diri dalam mengajarkan topik-topik keamanan siber kontemporer seperti penetration testing, analisis malware, dan forensika digital. Hal ini berimplikasi langsung pada kualitas pembelajaran yang diterima siswa.

Kesenjangan Infrastruktur Laboratorium

Tema kedua yang konsisten muncul adalah kesenjangan infrastruktur laboratorium. Yamin et al. (2021) dalam penelitian eksperimentalnya di Swiss mendemonstrasikan bahwa penggunaan cyber range lingkungan simulasi serangan dan pertahanan siber berbasis virtual secara signifikan meningkatkan kompetensi siswa TVET. Temuan ini menyoroti pentingnya infrastruktur pembelajaran yang relevan dengan praktik industri.

Dalam konteks Indonesia, studi Setiawan dan Wahyuningsih (2022) mengidentifikasi bahwa sebagian besar laboratorium komputer SMK masih didominasi oleh perangkat keras lama yang tidak mendukung penginstalan perangkat lunak keamanan siber yang dibutuhkan. Keterbatasan bandwidth internet di banyak sekolah juga menjadi hambatan dalam implementasi platform pembelajaran berbasis cloud yang semakin umum digunakan dalam pendidikan keamanan siber.

Ketidakresponsifan Kurikulum terhadap Perubahan Lanskap Ancaman
Manson dan Pike (2022) dalam survei nasional mereka di Amerika Serikat menemukan bahwa hanya 34% program pendidikan vokasi yang melakukan review kurikulum secara tahunan, sementara sisanya memiliki siklus review lebih dari tiga tahun. Mengingat rata-rata usia sebuah teknik serangan siber yang menjadi relevan dengan kurikulum adalah sekitar 18–24 bulan setelah kemunculannya, siklus review yang panjang menyebabkan kurikulum secara permanen tertinggal dari realitas ancaman yang dihadapi industri.

Fenomena ini diperparah oleh rigiditas birokrasi dalam pengembangan kurikulum formal. Di Indonesia, proses revisi Capaian Pembelajaran dan perangkat pembelajaran di SMK melibatkan berbagai pemangku kepentingan dan memerlukan waktu yang panjang, sehingga secara struktural sulit untuk merespons perubahan lanskap ancaman dengan kecepatan yang dibutuhkan.

Tema 2: Analisis Komparatif Kesesuaian Kurikulum TKJ dengan Standar Industri
Mengacu pada empat standar industri utama yang menjadi acuan penelitian ini, analisis komparatif mengungkap pola kesenjangan yang konsisten antara konten kurikulum TKJ dengan ekspektasi kompetensi yang ditetapkan standar industri.

Tabel 4. Pemetaan Kesenjangan Kurikulum TKJ terhadap Standar Industri Keamanan Siber

Standar Industri	Domain/Kompetensi Utama	Status dalam Kurikulum TKJ	Tingkat Kesenjangan	Rekomendasi Integrasi
NIST CSF 2.0 (2024)	Govern, Identify, Protect, Detect, Respond, Recover	Protect & Detect parsial; Govern, Respond, Recover sangat minimal	**TINGGI terutama pada fungsi Govern dan Respond**	Integrasi simulasi skenario insiden dan manajemen risiko dasar
CompTIA Security+ SY0-701 (2023)	Threats, Vulnerabilities, Security Architecture, Security Operations, Security Program Management	Security Architecture parsial; Security Operations dan Program Management hampir tidak ada	**TINGGI khususnya domain cloud security dan threat intelligence**	Adopsi modul CompTIA sebagai referensi pengembangan soal dan materi
Cisco CyberOps Associate	Security Concepts, Security Monitoring, Host-Based Analysis, Network Intrusion Analysis, Security Policies and Procedures	Security Concepts ada; Security Monitoring, Intrusion Analysis sangat minim	**SEDANG–TINGGI kesenjangan pada aspek monitoring dan analisis**	Adopsi Cisco NetAcad sebagai platform pembelajaran pelengkap
EC-Council CEH v12	Ethical Hacking, Footprinting, Scanning, Enumeration, Vulnerability Analysis, System Hacking	Hampir tidak tercakup dalam kurikulum TKJ saat ini	**SANGAT TINGGI seluruh domain tidak terwakili**	Integrasi konsep dasar ethical hacking sebagai enrichment program

Sumber: Dikembangkan oleh penulis berdasarkan analisis dokumen standar NIST (2024), CompTIA (2023), Cisco (2024), EC-Council (2023), dan Kurikulum Merdeka TKJ (Kemendikbudristek, 2022)

Tabel 4 menunjukkan bahwa kesenjangan terbesar terdapat pada aspek-aspek yang bersifat operasional dan taktis seperti security operations, incident response, dan ethical hacking sementara aspek-aspek yang lebih konseptual dan fundamental mendapatkan perhatian yang lebih memadai dalam kurikulum TKJ. Pola ini mencerminkan orientasi kurikulum yang lebih teoritis dibandingkan dengan keterampilan siap kerja yang dibutuhkan industri.

Tema 3: Hambatan Struktural Implementasi
Dimensi Kebijakan dan Regulasi
Beberapa artikel mengidentifikasi bahwa desain kebijakan pendidikan vokasi memiliki dampak signifikan terhadap kemampuan institusi TVET untuk mengadopsi standar industri keamanan siber. Andoh-Quainoo et al. (2022) dalam studi mereka di Ghana menemukan bahwa kebijakan yang mensyaratkan kemitraan industri formal sebagai prasyarat pembaruan kurikulum terbukti meningkatkan relevansi konten pendidikan. Studi dari

Chaudhary et al. (2023) mengidentifikasi bahwa kebijakan yang memberikan otonomi lebih besar kepada institusi TVET dalam adaptasi kurikulum menghasilkan respons yang lebih cepat terhadap perubahan kebutuhan industri.

Dimensi Kemitraan Industri

Toreini et al. (2020) menegaskan bahwa kemitraan yang bermakna antara institusi TVET dengan industri bukan hanya tentang penempatan magang (internship), melainkan mencakup partisipasi industri dalam desain kurikulum, penyediaan mentor dari praktisi, dan akses terhadap lingkungan kerja nyata. Studi mereka di Inggris menunjukkan bahwa program TVET dengan kemitraan industri yang terstruktur menghasilkan lulusan dengan tingkat kesesuaian kompetensi 40% lebih tinggi dibandingkan program tanpa kemitraan semacam itu.

Analisis Komparatif Kritis

Berdasarkan sintesis literatur, penelitian ini membandingkan empat aspek utama dalam pendidikan kejuruan di bidang Teknik Komputer dan Jaringan (TKJ). Dari sisi kapasitas guru, ditemukan bahwa 73,8% studi mengidentifikasi defisit kompetensi guru sebagai hambatan utama; meskipun program CPD berbasis sertifikasi industri terbukti efektif, keberlanjutannya sangat tergantung pada pendanaan yang konsisten, sehingga bagi TKJ direkomendasikan untuk memprioritaskan pelatihan guru dengan sertifikasi industri terakreditasi. Dalam hal infrastruktur, pemanfaatan virtual cyber range dan solusi berbasis cloud dinilai efektif mengatasi keterbatasan perangkat keras, namun masih membutuhkan bandwidth memadai dan komitmen langganan, sehingga TKJ disarankan mengadopsi platform virtual lab seperti Packet Tracer atau GNS3. Mengenai relevansi kurikulum, siklus review yang panjang menyebabkan ketertinggalan sistematis, sementara pendekatan modular memungkinkan pembaruan parsial tanpa restrukturisasi total, dengan implikasi bagi TKJ untuk menerapkan sistem kurikulum modular yang memisahkan komponen inti dan elektif. Terakhir, kemitraan industri terstruktur terbukti meningkatkan relevansi kompetensi lulusan hingga 40%, dengan model dual system ala Jerman yang efektif meskipun menghadapi tantangan regulasi di negara berkembang; oleh karena itu, TKJ perlu mengembangkan MoU berbasis kompetensi dengan perusahaan.

Tabel 5. Analisis Komparatif Temuan Penelitian

Aspek	Temuan Utama	Kelebihan Pendekatan Ada	Keterbatasan	Implikasi bagi TKJ
Kapasitas Guru	73,8% studi melaporkan defisit kompetensi guru sebagai hambatan utama	Beberapa program CPD (Continuing Professional Development) berbasis sertifikasi industri terbukti efektif	Keberlanjutan CPD bergantung pada pembiayaan yang konsisten	Prioritaskan program pelatihan guru berbasis sertifikasi industri terakreditasi
Infrastruktur	Virtual cyber range terbukti efektif mengatasi keterbatasan infrastruktur fisik	Solusi berbasis cloud dapat mengurangi biaya pengadaan hardware	Masih memerlukan bandwidth internet yang memadai dan komitmen langganan	Adopsi platform virtual lab (misalnya Packet Tracer, GNS3, cloud-based range)
Relevansi Kurikulum	Siklus review kurikulum yang panjang menyebabkan ketertinggalan sistematis	Modular curriculum design memungkinkan pembaruan parsial tanpa restrukturisasi total	Memerlukan mekanisme governance kurikulum yang lebih fleksibel	Terapkan sistem kurikulum modular dengan komponen inti dan elektif yang dapat diperbarui
Kemitraan Industri	Kemitraan terstruktur meningkatkan relevansi kompetensi lulusan hingga 40%	Model dual system (seperti di Jerman) terbukti efektif jika diimplementasikan dengan komitmen penuh	Implementasi di negara berkembang menghadapi tantangan regulatoris dan budaya organisasi	Kembangkan MoU berbasis kompetensi dengan perusahaan teknologi dan BUMN digital

Sumber: Dikembangkan oleh penulis berdasarkan sintesis literatur SLR

Peluang Integrasi Standar Industri Global dalam Kurikulum TKJ
Meskipun tantangan yang diidentifikasi cukup signifikan, analisis literatur juga mengungkap berbagai peluang yang dapat dimanfaatkan untuk menjembatani kesenjangan antara kurikulum TKJ dengan standar industri. Jones dan Pittman (2024) mengidentifikasi bahwa publikasi NIST CSF 2.0 pada 2024 membawa serta berbagai sumber daya pendidikan terbuka (open educational resources) yang dapat diadaptasi untuk berbagai level pendidikan, termasuk TVET.

Cisco Networking Academy, sebagai salah satu platform pendidikan teknologi terbesar di dunia dengan lebih dari 14.000 institusi mitra di 180 negara, menawarkan program beasiswa dan subsidi untuk institusi di negara berkembang. Program CyberOps Associate yang tersedia melalui platform ini selaras dengan kebutuhan kompetensi yang diidentifikasi dalam penelitian ini dan dapat diintegrasikan sebagai komplemen kurikulum TKJ tanpa biaya yang signifikan.

Rahim et al. (2023) dalam studi mereka di Malaysia menawarkan model integrasi bertahap yang dapat menjadi referensi bagi Indonesia. Model ini membagi integrasi standar industri ke dalam tiga fase: (1) Phase alignment memetakan dan menyelaraskan konten kurikulum yang ada dengan kerangka standar industri; (2) Phase enrichment menambahkan modul-modul komplementer berbasis standar industri; dan (3) Phase transformation meredesain kurikulum secara menyeluruh berdasarkan kerangka standar industri yang dipilih.

Implikasi bagi Pengembangan Kurikulum TVET Indonesia
Sintesis temuan dari 42 artikel yang dianalisis, dikontekstualisasikan dengan kondisi spesifik pendidikan vokasi Indonesia, menghasilkan serangkaian implikasi praktis yang dapat menjadi acuan bagi pengembangan kurikulum TKJ. Pertama, perlu dikembangkan mekanisme kemitraan kurikulum yang lebih terstruktur antara SMK TKJ dengan industri keamanan siber, bukan sekadar kemitraan magang. Kedua, program pengembangan profesional guru TKJ di bidang keamanan siber perlu diprioritaskan, dengan memanfaatkan skema sertifikasi industri yang tersedia dan diakui (seperti CompTIA Security+ atau Cisco CyberOps).

Ketiga, adopsi platform pembelajaran virtual dapat menjadi solusi pragmatis atas keterbatasan infrastruktur fisik; platform seperti Cisco Packet Tracer (tersedia gratis), GNS3 (open source), dan berbagai platform CTF yang bersifat freemium dapat diintegrasikan ke dalam pembelajaran TKJ tanpa investasi infrastruktur yang besar. Keempat, mekanisme pembaruan kurikulum perlu direformasi agar lebih responsif misalnya melalui sistem suplemen kurikulum yang dapat diperbarui secara mandiri oleh sekolah dalam batas-batas yang ditetapkan pusat.

Arah Penelitian Masa Depan
Berdasarkan sintesis literatur dan identifikasi gap penelitian, terdapat setidaknya lima arah penelitian yang direkomendasikan untuk mengisi celah pengetahuan yang masih ada. Pertama, studi empiris longitudinal yang mengukur dampak program pengembangan profesional guru TKJ berbasis sertifikasi industri terhadap kualitas pembelajaran dan kompetensi siswa. Kedua, pengembangan dan validasi model kurikulum TKJ adaptif yang dapat diperbarui secara modular tanpa memerlukan revisi kurikulum total.

Ketiga, penelitian aksi tentang implementasi platform virtual cyber range dalam konteks SMK Indonesia, termasuk analisis efektivitas, hambatan, dan faktor-faktor keberhasilan implementasinya. Keempat, studi komparatif antara model kemitraan industri-TVET dalam konteks keamanan siber di berbagai negara ASEAN untuk menghasilkan best practices yang kontekstual. Kelima, pengembangan dan validasi instrumen pengukuran kesesuaian kompetensi lulusan TKJ dengan kebutuhan industri keamanan siber yang dapat digunakan secara reguler.

Simpulan

Penelitian ini telah berhasil mensintesis 42 artikel ilmiah dari database Scopus, Web of Science, dan Google Scholar melalui pendekatan Systematic Literature Review berbasis protokol PRISMA 2020 untuk mengidentifikasi dan menganalisis tantangan implementasi keamanan siber dalam kurikulum Teknik Komputer dan Jaringan (TKJ) di SMK Indonesia. Temuan utama penelitian ini mereveal empat tantangan fundamental yang saling berkaitan: (1) defisit kapasitas pedagogis guru dalam materi keamanan siber yang kontemporer; (2) kesenjangan infrastruktur laboratorium yang tidak memadai untuk pembelajaran keamanan siber berbasis industri; (3) rigiditas mekanisme pembaruan kurikulum yang menyebabkan ketertinggalan sistematis dari perkembangan ancaman siber; dan (4) lemahnya kemitraan struktural antara SMK dengan industri dalam pengembangan kurikulum berbasis kompetensi. Analisis komparatif antara kurikulum TKJ dengan empat standar industri utama (NIST CSF 2.0, CompTIA Security+ SY0-701, Cisco CyberOps Associate, dan EC-Council CEH v12) menunjukkan kesenjangan yang signifikan terutama pada domain operasional keamanan siber seperti security operations, incident response, threat intelligence, dan ethical hacking sementara domain

konseptual mendapatkan perhatian yang lebih memadai. Kontribusi utama penelitian ini adalah tersedianya kerangka konseptual integrasi standar industri ke dalam kurikulum TVET yang mempertimbangkan secara simultan dimensi konten, pedagogi, kapasitas guru, infrastruktur, dan kemitraan industri. Kerangka ini diharapkan dapat menjadi acuan empiris bagi pengambil kebijakan pendidikan vokasi di Indonesia, khususnya dalam konteks revisi dan penguatan kurikulum TKJ dalam era Kurikulum Merdeka. Penelitian ini memiliki beberapa keterbatasan yang perlu diakui. Pertama, studi spesifik yang berfokus pada konteks Indonesia masih sangat terbatas dalam corpus literatur internasional, sehingga generalisasi temuan dari konteks lain perlu dilakukan dengan kehati-hatian. Kedua, analisis tematik yang digunakan memiliki unsur interpretasi subjektif meskipun telah diupayakan meminimalkannya melalui pengkodean oleh lebih dari satu peneliti. Ketiga, penelitian ini bersifat review dan belum menghasilkan data empiris primer dari konteks TKJ Indonesia secara langsung, sehingga studi lanjutan berbasis data primer sangat direkomendasikan.

References

Ahmad, R., & Yunos, Z. (2021). A dynamic cyber terrorism framework for cybersecurity. International Journal of Computer Science and Information Security, 19(3), 14–21.

Andoh-Quainoo, L., & Dzogbenuku, R. K. (2022). Industry-TVET partnerships for cybersecurity education in developing economies: Evidence from Ghana. International Journal of TVET Research, 8(2), 112–129.

Balitbang Kemendikbud. (2021). Laporan survei kompetensi guru SMK bidang teknologi informasi dan komunikasi. Pusat Penelitian Kebijakan, Kemendikbudristek.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bresniker, K., Gavrilovska, A., Holt, J., Milojicic, D., & Tran, T. (2021). Grand challenge: Applying artificial intelligence and machine learning to cybersecurity. Computer, 52(12), 45–52. https://doi.org/10.1109/MC.2019.2948846

BSSN. (2022). Laporan tahunan keamanan siber nasional 2022. Badan Siber dan Sandi Negara Republik Indonesia.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). Developing workforce skills in cybersecurity for TVET in South Asian contexts: Challenges and opportunities. Computers & Security, 126, 103064. https://doi.org/10.1016/j.cose.2022.103064

Cisco. (2024). Cisco CyberOps Associate certification curriculum overview. Cisco Networking Academy. https://www.netacad.com/courses/cybersecurity

CompTIA. (2023). CompTIA Security+ (SY0-701) exam objectives. CompTIA. https://www.comptia.org/certifications/security

Crick, T., & Knight, C. (2023). Addressing the cybersecurity skills gap: From the classroom to the boardroom.
IEEE Security & Privacy, 21(1), 78–83. https://doi.org/10.1109/MSEC.2022.3221975

Cybersecurity Ventures. (2023). 2023 official cybercrime report. Cybersecurity Ventures.

Direktorat SMK Kemendikbudristek. (2022). Data pokok pendidikan menengah kejuruan 2021/2022. Direktorat Sekolah Menengah Kejuruan.

EC-Council. (2023). Certified Ethical Hacker (CEH v12) program overview. EC-Council. https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

European Union Agency for Cybersecurity (ENISA). (2022). European Cybersecurity Skills Framework (ECSF). Publications Office of the European Union. https://doi.org/10.2824/786743

Furnell, S., & Bishop, M. (2020). Addressing cyber security skills: The spectrum, not the silo. Computer Fraud & Security, 2020(2), 6–11. https://doi.org/10.1016/S1361-3723(20)30012-1

Gough, D., Oliver, S., & Thomas, J. (Eds.). (2017). An introduction to systematic reviews (2nd ed.). SAGE Publications.

ISC². (2023). ISC² cybersecurity workforce study 2023. ISC². https://www.isc2.org/Research/Workforce-Study

Jones, R., & Pittman, J. (2024). NIST Cybersecurity Framework 2.0: Implications for vocational education curriculum design. Journal of Cybersecurity Education, Research and Practice, 2024(1), Article 3.

Kemendikbudristek. (2022). Capaian pembelajaran pada pendidikan vokasi: Program keahlian Teknik Komputer dan Jaringan. Pusat Kurikulum dan Pembelajaran.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2023). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1–10. https://doi.org/10.3233/THC-161263

Lim, M., Abdullah, A., & Jhanjhi, N. Z. (2022). Performance optimization of criminal network hidden link prediction model with deep reinforcement learning. Journal of King Saud University–Computer and Information Sciences, 34(5), 1992–2003.

Manson, D., & Pike, R. (2022). Cybersecurity curriculum review cycles in vocational education: A national survey. Journal of Information Systems Education, 33(3), 180–193.

Merkow, M. S., & Breithaupt, J. (2023). Information security: Principles and practice (3rd ed.). Pearson Education.

Montaño, J., Yamin, M., & Katt, B. (2022). Effectiveness of cyber range-based training for vocational cybersecurity education. Computers & Education, 186, 104525. https://doi.org/10.1016/j.compedu.2022.104525

National Institute of Standards and Technology (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST. https://doi.org/10.6028/NIST.CSWP.29

NICE. (2023). NICE Cybersecurity Workforce Framework (NIST SP 800-181r1). National Initiative for Cybersecurity Education, NIST. https://doi.org/10.6028/NIST.SP.800-181r1

Paganini, P., & Jones, R. (2023). Cybersecurity education frameworks: Bridging the gap between academic knowledge and industry needs. Information & Computer Security, 31(2), 177–195.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Rahim, N. H. A., Hamid, S., & Mat Kiah, M. L. (2023). Cybersecurity competency alignment between TVET curriculum and CompTIA Security+ in Malaysia: A mixed-methods study. Journal of Technical Education and Training, 15(3), 45–63.

Salihu, A., & Abdullahi, S. (2022). Integrating cybersecurity into technical and vocational education and training: Prospects and challenges. Education and Information Technologies, 27(6), 7891–7917. https://doi.org/10.1007/s10639-022-10941-z

Setiawan, B., & Wahyuningsih, D. (2022). Analisis kesiapan kurikulum dan guru TKJ SMK dalam mengajarkan kompetensi keamanan jaringan berbasis standar industri. Jurnal Pendidikan Vokasi, 12(2), 134–148. https://doi.org/10.21831/jpv.v12i2.48532

SkillsFuture Singapore. (2023). Skills framework for infocomm technology: Cybersecurity. SkillsFuture Singapore. https://www.skillsfuture.gov.sg/skills-framework/ict

Talib, S., Clarke, N. L., & Furnell, S. M. (2022). An analysis of information security awareness within home and work environments. International Journal of Digital Society, 1(1), 54–63.

Toreini, E., Aitken, M., Coopamootoo, K., Elliott, K., Zelaya, C. G., & van Moorsel, A. (2020). The relationship between trust in AI and trustworthy machine learning technologies. Proceedings of FAT*, 272–283. https://doi.org/10.1145/3351095.3372834

UNESCO. (2021). Recommendation on open educational resources. UNESCO. https://en.unesco.org/about-us/legal-affairs/recommendation-open-educational-resources-oer

UNESCO-UNEVOC. (2022). Skills for work and life: TVET's role in building resilient communities. UNESCO-UNEVOC International Centre.

Wangen, G., Snekkenes, E., & Moraes, R. (2021). Cybersecurity capacity in higher education: Mapping the landscape. IEEE Access, 9, 95121–95136. https://doi.org/10.1109/ACCESS.2021.3094279

World Economic Forum. (2023). Future of jobs report 2023. World Economic Forum. https://www.weforum.org/reports/the-future-of-jobs-report-2023/

Yamin, M. M., Katt, B., & Gkioulos, V. (2021). Cyber ranges and security testbeds: Scenarios, functions, tools, and architecture. Computers & Security, 102, 102126. https://doi.org/10.1016/j.cose.2020.102126

Zheng, M., Bos, J., & Dent, A. (2022). Incorporating practical cybersecurity skills into vocational education: A case study of CTF-based learning in Singapore ITE. Computers & Education, 182, 104481.

Zubairi, J. A., & Mahboob, T. (2023). Emerging cybersecurity challenges for TVET institutions in the Global South. International Journal of Educational Technology in Higher Education, 20(1), 15. https://doi.org/10.1186/s41239-023-00382-0

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269.