Kontribusi Kompetensi Keamanan Jaringan Berbasis STEM terhadap Kemandirian dan Keunggulan Kompetitif Mahasiswa Era 4.0

Lisa Rahma Aulia Putri[1], Satria Bagus Putra Hermawan[2], Arrori Ashar Hidayad[3], Boedy Irhadtanto[4]

[1,2,3,4]Pendidikan Teknologi Informasi, IKIP PGRI Bojonegoro,
Jl. Panglima Polim No. 46, Klangon, Kec. Bojonegoro, Kab. Bojonegoro, Jawa Timur 62114.
E-mail: lisarahmaauliaputri@gmail.com[1], satriabagusputra07@gmail.com[2,]
arroriasharhidayad17@gmail.com[3] , boedyirh@ikippgribojonegoro.ac.id[4]
Telp: +0895618360606[1] , +62 895-6218-05656 [2], +6285895446352[3], +6285730262105[4]

Abstrak

Era Industri 4.0 mendorong transformasi digital yang pesat sekaligus meningkatkan ancaman keamanan siber dan kebutuhan tenaga profesional di bidang tersebut. Penelitian ini bertujuan untuk menganalisis kontribusi kompetensi keamanan jaringan berbasis STEM terhadap kemandirian belajar dan keunggulan kompetitif mahasiswa. Metode penelitian yang digunakan adalah studi pustaka dengan pendekatan kualitatif deskriptif melalui analisis berbagai literatur ilmiah terbitan tahun 2020–2025. Hasil penelitian menunjukkan bahwa kompetensi keamanan jaringan berbasis STEM tidak hanya memperkuat kemampuan teknis mahasiswa, tetapi juga mengembangkan keterampilan berpikir kritis, pemecahan masalah, kolaborasi, dan pembelajaran mandiri. Pendekatan pembelajaran berbasis STEM melalui Problem-Based Learning (PBL), Challenge-Based Learning (CBL), dan aktivitas praktik keamanan siber terbukti mendukung peningkatan kemandirian mahasiswa. Selain itu, kompetensi tersebut memberikan keunggulan kompetitif karena selaras dengan kebutuhan industri terhadap tenaga kerja yang adaptif dan siap menghadapi tantangan keamanan digital. Penelitian ini menyimpulkan bahwa kompetensi keamanan jaringan berbasis STEM berkontribusi signifikan dalam membentuk mahasiswa yang mandiri, kompeten, dan berdaya saing di era Industri 4.0.

Kata Kunci: kompetensi keamanan jaringan, STEM, kemandirian mahasiswa, keunggulan kompetitif, Industri 4.0

Abstract

The Industry 4.0 era is driving rapid digital transformation while simultaneously increasing cybersecurity threats and the demand for professionals in this field. This study aims to analyze the contribution of STEM-based network security competencies to students' self-directed learning and competitive advantage. The research method employed is a literature review using a descriptive qualitative approach through the analysis of various scientific publications from 2020–2025. The results indicate that STEM-based network security competencies not only strengthen students' technical skills but also develop critical thinking, problem-solving, collaboration, and self-directed learning skills. STEM-based learning approaches, such as Problem-Based Learning (PBL), Challenge-Based Learning (CBL), and cybersecurity practical activities, have been proven to support the enhancement of students' self-directed learning. Furthermore, these competencies provide a competitive edge as they align with industry needs for an adaptive workforce ready to face digital security challenges. This study concludes that STEM-based network security competencies significantly contribute to shaping students who are independent, competent, and competitive in the Industry 4.0 era.

Keywords: *network security competency, STEM, student independence, competitive advantage, Industry 4.0*

PENDAHULUAN

Era Industri 4.0 telah membawa transformasi fundamental dalam lanskap ekonomi global melalui adopsi teknologi-teknologi canggih seperti kecerdasan buatan (*artificial intelligence*), komputasi awan (*cloud computing*), *Internet of Things* (IoT), dan big data. Pemerintah dan bisnis di seluruh dunia mengadopsi teknologi Revolusi Industri 4.0 untuk meningkatkan efisiensi, daya saing, dan inovasi. Namun transformasi digital yang sama yang memungkinkan pertumbuhan ini juga memicu peningkatan ancaman keamanan siber yang tidak dapat diabaikan oleh industri mana pun

(Alkadrie & Fitroh, 2024). Serangan siber modern, termasuk ransomware, *phishing*, pelanggaran data, dan *distributed denial-of-service* (DDoS), telah meningkat secara signifikan, dengan kejahatan siber (Alkadrie & Fitroh, 2024).

Di tengah meningkatnya ancaman ini, dunia menghadapi kesenjangan talenta keamanan siber yang kritis. Kebutuhan untuk profesi teknologi keamanan mencapai 350% dari tahun 2013 hingga 2021. dan bahkan dengan perekrutan yang intensif, diproyeksikan masih akan ada kesenjangan 3,5 juta pada tahun 2021 (Cornelius dkk., 2021: 2). Di Inggris, survei terbaru menunjukkan bahwa 49% bisnis memiliki kesenjangan keterampilan teknis keamanan siber dasar, sementara 30% bisnis memiliki kesenjangan keterampilan teknis tingkat lanjut, dan dampak dari kurangnya keterampilan teknis di kalangan karyawan yang ada telah meningkat tahun demi tahun. Kesenjangan talenta ini sebagian disebabkan oleh pendekatan pendidikan tradisional yang belum sepenuhnya siap memenuhi tuntutan industri, di mana banyak lulusan meninggalkan universitas dengan keterampilan teknis yang kuat tetapi masih kurang dalam keterampilan keamanan siber yang diperlukan industri. Era teknologi canggih yang ditandai dengan inovasi seperti jaringan 6G dan lingkungan multi-cloud menuntut perlindungan infrastruktur siber yang sangat penting, namun eskalasi ancaman siber secara simultan telah mengekspos kekurangan signifikan dalam keahlian keamanan siber (Blažič, 2022:2).

Dalam konteks inilah pendekatan STEM (*Science, Technology, Engineering, Mathematics*) muncul sebagai kerangka kerja yang menjanjikan untuk mempersiapkan mahasiswa menghadapi tantangan keamanan siber. Mengintegrasikan prinsip-prinsip keamanan siber, kecerdasan buatan, dan IoT ke dalam kurikulum STEM sangat penting untuk mempersiapkan pemimpin dan profesional masa depan, karena kerangka kerja semacam itu tidak hanya membekali mahasiswa dengan kompetensi yang diperlukan untuk menavigasi dan mengamankan lingkungan digital yang saling terhubung, tetapi juga mempersiapkan mereka dengan seperangkat keterampilan yang mereka butuhkan untuk menavigasi lanskap digital kehidupan nyata. Selain itu, kerangka kerja ini membantu mahasiswa mengembangkan pola pikir langsung di bidang keamanan sekaligus menyoroti peluang yang dimiliki oleh kecerdasan buatan, teknologi pintar, dan teknologi berkembang lainnya (Blažič, 2022:3).

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis bagaimana kontribusi kompetensi keamanan jaringan yang dibangun melalui pendekatan STEM terhadap terciptanya kemandirian belajar dan keunggulan kompetitif mahasiswa di era Industri 4.0, dengan ruang lingkup kajian pada kompetensi keamanan jaringan dalam kerangka STEM serta indikator kemandirian dan keunggulan kompetitif mahasiswa program studi teknologi informasi dan komputer.

METODE

Penelitian ini menggunakan desain studi pustaka (library research) dengan pendekatan kualitatif deskriptif. Metode ini dipilih karena penelitian bertujuan untuk menganalisis secara mendalam kontribusi kompetensi keamanan jaringan berbasis STEM terhadap kemandirian dan keunggulan kompetitif mahasiswa di era Industri 4.0 berdasarkan kajian terhadap literatur yang relevan (Amir dkk., 2023:308). Melalui pendekatan kualitatif, peneliti dapat memperoleh pemahaman holistik tentang motif, praktik, dan faktor-faktor yang mempengaruhi efektivitas pendidikan keamanan siber berbasis STEM. Sumber data penelitian ini berasal dari artikel, jurnal ilmiah, serta laporan resmi lembaga pemerintah dan industri. Kriteria inklusi sumber meliputi: dipublikasikan tahun 2020-2025, relevan dengan topik STEM dan keamanan siber, tersedia teks lengkap, serta berasal dari sumber terakreditasi.

Prosedur pengumpulan data dilaksanakan melalui tiga tahap. Tahap pertama, pencarian literatur pada basis data Google Scholar, dan repositori institusi menggunakan kata kunci seperti "STEM cybersecurity education", "network security competency", dan "Industry 4.0 skills gap". Tahap kedua, penyaringan artikel berdasarkan judul, abstrak, dan relevansi. Tahap ketiga, ekstraksi

data dengan mencatat penulis, tahun, sumber, halaman, dan kutipan spesifik yang relevan (Fadli, 2021:35).

Teknik analisis data yang digunakan adalah analisis isi (content analysis) dengan pendekatan tematik melalui empat langkah: reduksi data, penyajian data, verifikasi sumber, dan penarikan kesimpulan. Sebagaimana dijelaskan dalam penelitian tentang kesadaran keamanan siber, analisis data kualitatif dilakukan dengan mengidentifikasi tema-tema utama seperti metode perlindungan, kesadaran, dan kompetensi teknis (Fadli, 2021:35).

Keabsahan data dijamin melalui kredibilitas dengan menggunakan beragam sumber terakreditasi dan konfirmabilitas dengan mencantumkan kutipan langsung serta referensi halaman dari setiap sumber, sehingga pembaca dapat melacak kembali temuan ke sumber aslinya (Fadli, 2021:35)

HASIL DAN PEMBAHASAN

Kompetensi Keamanan Jaringan dalam Kerangka STEM

Pendidikan keamanan siber berbasis STEM mengalami perkembangan yang signifikan dalam beberapa tahun terakhir. Perkembangan ini didorong oleh meningkatnya kebutuhan industri terhadap tenaga profesional yang memiliki kemampuan teknis sekaligus keterampilan berpikir kritis dalam menghadapi ancaman siber yang semakin kompleks. Meskipun berbagai institusi pendidikan telah meningkatkan investasi pada kursus, platform digital, dan lingkungan pembelajaran keamanan siber, kesenjangan keterampilan masih menjadi tantangan utama dalam pendidikan tinggi (Blažič, 2022:3).

Berbagai kerangka pendidikan keamanan siber internasional, seperti European Cybersecurity Skills Framework dan NIST/NICE Framework, menunjukkan bahwa kompetensi profesional di bidang keamanan siber tidak hanya mencakup kemampuan teknis, tetapi juga keterampilan lintas bidang yang mendukung kesiapan kerja mahasiswa (Mukherjee dkk., 2024:2). Kompetensi teknis tersebut meliputi keamanan jaringan, keamanan sistem operasi, keamanan komunikasi web, keamanan perangkat mobile dan IoT, serta pemahaman logika sistem. Di sisi lain, kompetensi transversal seperti critical thinking, problem solving, teamwork, lifelong learning, dan ethical thinking juga dinilai sangat penting dalam membentuk profesional keamanan siber yang adaptif.

Temuan tersebut menunjukkan bahwa pendekatan STEM mampu membangun kompetensi keamanan jaringan secara lebih komprehensif dibandingkan pembelajaran konvensional yang hanya berfokus pada aspek teoritis. Pendekatan ini memungkinkan mahasiswa mengintegrasikan kemampuan analitis, logika, dan keterampilan teknis melalui proses pembelajaran yang kontekstual dan berbasis pemecahan masalah. Dengan demikian, mahasiswa tidak hanya memahami konsep keamanan jaringan secara teoritis, tetapi juga mampu menerapkannya dalam situasi nyata.

Selain itu, penelitian mengenai Cybersecurity Education Maturity Model (CEMM) menunjukkan bahwa kualitas pendidikan keamanan siber di perguruan tinggi sangat dipengaruhi oleh kesiapan institusi dalam menyediakan kurikulum, fasilitas, dan tenaga pengajar yang kompeten (Kreider & Almalag, 2020:1). Hal ini menunjukkan bahwa penguatan kompetensi keamanan jaringan berbasis STEM membutuhkan dukungan institusi yang berkelanjutan agar mampu menghasilkan lulusan yang relevan dengan kebutuhan industri digital.

Kontribusi terhadap Kemandirian Mahasiswa

Hasil kajian menunjukkan bahwa pendekatan pembelajaran berbasis STEM memberikan kontribusi signifikan terhadap pembentukan kemandirian mahasiswa. Model pembelajaran aktif seperti Problem-Based Learning (PBL) dan Challenge-Based Learning (CBL) mendorong mahasiswa untuk terlibat secara langsung dalam proses pemecahan masalah, pengambilan keputusan, dan eksplorasi teknologi secara mandiri.

Dalam konteks pendidikan keamanan siber, pendekatan PBL terbukti mampu meningkatkan agensi mahasiswa dalam memahami dan menyelesaikan persoalan keamanan jaringan yang kompleks. Penelitian Park dkk. (2023:1) menunjukkan bahwa mahasiswa yang memiliki meta-agency yang baik cenderung lebih mampu mengatur proses belajar secara mandiri, memahami tantangan pembelajaran, serta menentukan strategi penyelesaian masalah secara efektif. Kondisi tersebut memperlihatkan bahwa pembelajaran keamanan jaringan berbasis STEM tidak hanya meningkatkan kemampuan teknis, tetapi juga membentuk pola belajar mandiri yang sangat penting di era digital.

Kemandirian mahasiswa juga berkembang melalui keterlibatan dalam kompetisi keamanan siber dan aktivitas praktik di luar kurikulum formal. Program seperti CyberForce Competition memberikan pengalaman langsung kepada mahasiswa dalam menghadapi simulasi ancaman siber berbasis dunia kerja. Melalui kegiatan tersebut, mahasiswa memperoleh kesempatan untuk mengembangkan kemampuan analisis, investigasi digital, forensik, serta pengambilan keputusan dalam situasi nyata (Argonne National Laboratory, 2024).

Partisipasi dalam kompetisi keamanan siber juga memperlihatkan bahwa mahasiswa terdorong untuk belajar secara aktif di luar materi yang diperoleh di kelas. Kondisi ini menunjukkan bahwa pembelajaran berbasis STEM mampu menciptakan lingkungan belajar yang mendorong mahasiswa menjadi pembelajar mandiri, adaptif, dan memiliki inisiatif tinggi dalam meningkatkan kompetensi profesional mereka.

Keunggulan Kompetitif di Era Industri 4.0

Analisis mengenai keunggulan kompetitif menunjukkan bahwa lulusan dengan kompetensi keamanan jaringan berbasis STEM memiliki posisi tawar yang tinggi di pasar kerja. Laporan ISC2 dalam (Argonne National Laboratory, 2024) menunjukkan bahwa kesenjangan tenaga kerja keamanan siber global mencapai 4.763.963 orang. Selain itu, pertumbuhan tenaga kerja keamanan siber global mengalami perlambatan, sementara kebutuhan organisasi terhadap profesional keamanan siber terus meningkat. Laporan tersebut juga menunjukkan bahwa kesenjangan keterampilan (skills gap) berdampak signifikan terhadap kemampuan organisasi dalam menjaga keamanan sistem mereka.

Lebih dari 57% organisasi bertujuan untuk mengurangi kesenjangan ini dengan berinvestasi dalam pelatihan dan sertifikasi, namun penelitian menunjukkan bahwa masih ada kesenjangan yang jelas antara apa yang diharapkan oleh bisnis dan apa yang diberikan oleh pendidikan tinggi. Responden dari industri bisnis memberikan tingkat kepentingan sekitar 10% lebih tinggi pada keterampilan transversal dan profesional dibandingkan dengan sektor pendidikan (Goupil dkk., 2022:2). Peran paling sulit untuk diisi dalam industri keamanan siber meliputi *penetration tester*, *cybersecurity manager*, *network engineer*, *information security architect*, *cybersecurity researcher*, *application security tester*, *incident handling specialist*, dan *malware analyst*. Posisi-posisi ini menuntut kreativitas paling tinggi dan pengetahuan lintas bidang yang luas di banyak area, memerlukan persiapan yang komprehensif serta praktik yang ekstensif dan beragam (Pirta-Dreimane dkk., 2024:5).

Solusi yang diusulkan untuk mengatasi kesenjangan ini mencakup praktik langsung melalui simulasi kejadian dunia nyata, presentasi kasus nyata yang dilakukan oleh pemberi kerja di universitas, penyertaan skenario praktis yang ekstensif, magang wajib, serta kolaborasi antara universitas dan pemberi kerja dalam rangka pembentukan program. Peningkatan penekanan pada partisipasi aktif mahasiswa dalam lingkungan keamanan siber, penggunaan alat pelatihan sumber terbuka seperti *Hack the Box*, serta partisipasi dalam proyek sumber terbuka untuk memahami secara holistik keadaan industri juga menjadi rekomendasi penting (Angjelina & Riandi, 2023:87).

Penelitian tentang model pembelajaran *Challenge-Based Learning* (CBL) yang disinergikan dengan *Industry-in-Curriculum* (IIC) di Ngee Ann Polytechnic, Singapura, menunjukkan bahwa pendekatan ini berhasil menghasilkan keterlibatan mahasiswa yang tinggi, hasil Module Experience

Survey (MES) yang positif secara konsisten, serta transfer keterampilan yang dapat didemonstrasikan ke modul dan magang berikutnya. Model ini diterapkan dalam modul Network Security untuk mahasiswa diploma Cybersecurity & Digital Forensics dengan melibatkan 248 mahasiswa selama dua semester. Tantangan dirancang bersama dengan profesional industri dan mencerminkan tugas-tugas dunia nyata, yang mengharuskan mahasiswa bertindak sebagai arsitek keamanan yang bertugas merancang dan mempertahankan lingkungan jaringan tingkat perusahaan. Penggunaan alat profesional seperti *Palo Alto firewalls* dan pembelajaran berbasis flipped learning semakin memperdalam pemahaman mahasiswa (Vilalta-Perdomo dkk., 2022:2).

Tantangan Implementasi

Meskipun berbagai temuan menunjukkan dampak positif pendekatan STEM terhadap kompetensi dan daya saing mahasiswa, sejumlah tantangan implementasi tetap perlu diakui.Salah satu tantangan utama adalah keterbatasan infrastruktur laboratorium dan lingkungan praktik virtual yang memadai. Pembelajaran keamanan jaringan membutuhkan simulasi sistem, jaringan, dan ancaman siber yang kompleks sehingga memerlukan dukungan teknologi dan biaya yang tidak sedikit (Angjelina & Riandi, 2023:84).

Selain itu, perkembangan teknologi keamanan siber yang sangat cepat menyebabkan kurikulum perguruan tinggi sering mengalami ketertinggalan dibanding kebutuhan industri. Penelitian mengenai Cybersecurity Education Maturity Model menunjukkan bahwa perguruan tinggi perlu melakukan pembaruan kurikulum secara berkala agar kompetensi yang diajarkan tetap relevan dengan perkembangan dunia kerja (Mero & Pepsin, 2025:3).

Tantangan lainnya adalah keterbatasan tenaga pengajar yang memiliki kompetensi khusus di bidang keamanan siber. Pendidikan keamanan jaringan berbasis STEM membutuhkan dosen yang tidak hanya memahami teori, tetapi juga memiliki pengalaman praktik dan kemampuan mengikuti perkembangan teknologi keamanan digital secara berkelanjutan. Oleh karena itu, penguatan kualitas sumber daya manusia dan kolaborasi dengan industri menjadi aspek penting dalam keberhasilan implementasi pendidikan keamanan siber berbasis STEM (Mero & Pepsin, 2025:3).

Sintesis: Kontribusi terhadap Kemandirian dan Keunggulan Kompetitif

Berdasarkan seluruh temuan yang telah dipaparkan, dapat disintesis bahwa kompetensi keamanan jaringan berbasis STEM memberikan kontribusi ganda terhadap mahasiswa. Pertama, dari aspek kemandirian, pendekatan pembelajaran aktif seperti PBL, CBL, dan kompetisi keamanan siber terbukti efektif mengembangkan kemampuan mahasiswa untuk belajar secara mandiri dan mengambil inisiatif dalam memperdalam kompetensi di luar kurikulum formal. Kompetisi keamanan siber merupakan acara yang bermanfaat tidak hanya bagi mahasiswa, tetapi juga bagi para dosen/guru yang melalui acara tersebut memiliki kesempatan untuk mengaitkan teori dengan praktik, seiring dengan semakin kompleksnya tantangan keamanan siber yang melibatkan berbagai disiplin ilmu dan terkadang melampaui materi pelajaran yang dibahas di kelas (Pitman, 2024:3).

Kedua, dari aspek keunggulan kompetitif, lulusan dengan kompetensi keamanan jaringan berbasis STEM memiliki posisi yang lebih unggul di pasar kerja Dari aspek daya saing kerja, lulusan dengan kompetensi keamanan siber dan keterampilan teknis multidisiplin memiliki peluang yang lebih baik karena industri membutuhkan tenaga ahli yang menguasai jaringan komputer, perangkat lunak, sistem terintegrasi, dan manajemen keamanan (Kunicina dkk., 2020). (Kunicina dkk., 2020) menekankan pentingnya kolaborasi perguruan tinggi dengan perusahaan IT serta keterlibatan mahasiswa dalam proyek dan pekerjaan kontrak industri untuk memberikan pengalaman praktis dan meningkatkan kesiapan profesional lulusan. Dengan demikian, investasi dalam pengembangan kompetensi keamanan jaringan berbasis STEM merupakan strategi yang tepat bagi mahasiswa untuk memenangkan persaingan di era Industri 4.0.

SIMPULAN

Berdasarkan hasil kajian literatur dan pembahasan yang telah dilakukan mengenai kontribusi kompetensi keamanan jaringan berbasis STEM terhadap kemandirian dan keunggulan kompetitif mahasiswa di era Industri 4.0, dapat disimpulkan tiga hal utama.

Pertama, kompetensi keamanan jaringan dalam kerangka STEM mencakup integrasi keterampilan teknis (keamanan jaringan, sistem operasi, IoT, dan logika sistem) dengan keterampilan lintas bidang (pemikiran kritis, pemecahan masalah, kerja sama tim, pembelajaran seumur hidup, dan etika). Kerangka ini menjadi fondasi pengembangan kurikulum keamanan siber yang responsif terhadap tuntutan Industri 4.0, di mana universitas perlu secara bertahap meningkatkan penawaran keamanan siber dari kursus tunggal hingga program penuh.

Kedua, pendekatan STEM berkontribusi signifikan terhadap kemandirian belajar mahasiswa melalui metode Problem-Based Learning (PBL) dan Challenge-Based Learning (CBL) yang mempromosikan kemampuan memecahkan masalah kompleks secara mandiri. Partisipasi dalam kompetisi keamanan siber juga mendorong pembelajaran mandiri berkelanjutan di luar kurikulum formal, sementara teknologi laboratorium virtual mendukung akses praktik kapan saja.

Ketiga, kompetensi ini menciptakan keunggulan kompetitif yang nyata di pasar kerja. Di tengah kesenjangan talenta keamanan siber global yang mencapai hampir 4,8 juta orang, lulusan dengan keterampilan teknis terbukti dan keterampilan lintas bidang yang kuat memiliki posisi tawar lebih tinggi, terutama untuk peran-peran kunci seperti penguji penetrasi, manajer keamanan siber, dan insinyur jaringan.

Secara keseluruhan, kompetensi keamanan jaringan berbasis STEM memberikan kontribusi ganda yang saling memperkuat: kemandirian belajar mendorong peningkatan kompetensi berkelanjutan, yang pada gilirannya memperkuat keunggulan kompetitif, sementara kesadaran akan tuntutan industri memotivasi mahasiswa untuk lebih mandiri dalam belajar.

Rekomendasi penelitian ini meliputi: bagi institusi pendidikan, disarankan mengadopsi model kematangan pendidikan keamanan siber dan memperkuat kolaborasi industri; bagi mahasiswa, disarankan aktif berpartisipasi dalam kompetisi dan memanfaatkan platform pelatihan sumber terbuka; bagi pembuat kebijakan, disarankan mendukung pendanaan laboratorium virtual dan skema sertifikasi yang diakui industri. Penelitian lebih lanjut diperlukan untuk mengkaji implementasi model-model ini secara empiris dalam konteks Indonesia.

DAFTAR PUSTAKA

Alkadrie, S. A. & Fitroh. (2024). Keamanan Cloud Computing di Era Industri 4.0: Systematic Literature Review. *KONSTELASI: Konvergensi Teknologi dan Sistem Informasi*, *4*(2). https://doi.org/10.24002/konstelasi.v4i2.10277

Amir, D. R., Zahro, F. S., Puspitanigsih, S., & Fawaid, M. I. (2023). Efektifitas Penggunaan Wodershare Filmora dalam Editing Video Pada Pembelajaran Pengantar Teknologi Informasi. *Prosiding Seminar Nasional Pendidikan FPMIPA*, 306–313.

Angjelina, P., & Riandi, R. (2023). Analisis Literatur: Aspek-Aspek Positif dan Keterbatasan Pembelajaran STEM. *Natural: Jurnal Ilmiah Pendidikan IPA*, *10*(2), 83–91. https://doi.org/10.30738/natural.v10i2.15304

Argonne National Laboratory. (2024). University students tackle Adventure in CyberForce. *EurekAlert*. https://www.eurekalert.org/news-releases/1044647

Blažič, B. J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies*, *27*(3), 3011–3036. https://doi.org/10.1007/s10639-021-10704-y

Cornelius, A., Crouch, A., Macatuno, F., Jackson, M., Johnson, W., & Haderlie, D. (2021). *Understanding How Organizations Handle Cybersecurity* (INL/EXT-21-64319-Rev000, 1836041; hlm. INL/EXT-21-64319-Rev000, 1836041). https://doi.org/10.2172/1836041

Fadli, M. R. (2021). *Memahami desain metode penelitian kualitatif*. *21*(1), 33–54.

Goupil, F., Laskov, P., Pekaric, I., Felderer, M., Dürr, A., & Thiesse, F. (2022). Towards Understanding the Skill Gap in Cybersecurity. *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1*, 477–483. https://doi.org/10.1145/3502718.3524807

Kreider, C., & Almalag, M. (2020). *Quantifying Program Offerings with a Cybersecurity Education Maturity Model*. 1–2.

Kunicina, N., Zabasta, A., Krumins, O., Romanovs, A., & Patlins, A. (2020). Cybersecurity Curricula Recommendations Development for Technical Background and Engineering Skills in International Dimension. *2020 IEEE 61th International Scientific Conference on Power and Electrical Engineering of Riga Technical University (RTUCON)*, 1–6. https://doi.org/10.1109/RTUCON51174.2020.9316573

Mero, P., & Pepsin, A. (2025). *ASSESSING THE MATURITY OF CYBERSECURITY EDUCATION IN VIRGINIA AND IMPACT OF STATE LEVEL INVESTMENT*. https://doi.org/https://doi.org/10.48550/arXiv.2502.18456

Mukherjee, M., Le, N. T., Chow, Y.-W., & Susilo, W. (2024). Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information*, *15*(2), 117. https://doi.org/10.3390/info15020117

Park, J., Deng, Y., Agrawal, G., Techawitthayachinda, R. I., Chen, Y.-C., Huang, D., & Liu, H. (2023). Problems of Problem-Based Learning: Exploring Meta-Agency in Problem-Based Cybersecurity Learning in College Education. *Proceedings of the 2023 AERA Annual Meeting*. 2023 AERA Annual Meeting. https://doi.org/10.3102/2017777

Pirta-Dreimane, R., Romanovs, A., Bikovska, J., Pekša, J., Vartiainen, T., Valliou, M., Kamsamrong, J., & Eltahawy, B. (2024). Enhancing Smart Grid Resilience: An Educational Approach to Smart Grid Cybersecurity Skill Gap Mitigation. *Energies*, *17*(8), 1876. https://doi.org/10.3390/en17081876

Pitman, L. (2024). Solving the Cybersecurity Challenge: Students' and Educators' Views on Cybersecurity Competitions. *International Journal of Cyber Research and Education*, *5*(1), 1–14. https://doi.org/10.4018/IJCRE.351643

Vilalta-Perdomo, E., Michel-Villarreal, R., & Thierry-Aguilera, R. (2022). Integrating Industry 4.0 in Higher Education Using Challenge-Based Learning: An Intervention in Operations Management. *Education Sciences*, *12*(10), 663. https://doi.org/10.3390/educsci12100663