

ANCAMAN SIBER DAN URGENSI PENDIDIKAN KARAKTER BAGI GENERASI MUDA: PERSPEKTIF DIGITAL CITIZENSHIP DALAM MEMBANGUN WARGA NEGARA DIGITAL YANG BERINTEGRITAS

Dini Oktariani¹, Dedek Helida Pitra²

Universitas Bangka Belitung¹

Universitas Muhammadiyah Muara Bungo²

*Korespondensi: Dini-oktariani@ubb.ac.id

Abstrak

Transformasi digital telah memberikan berbagai manfaat bagi kehidupan masyarakat, namun di sisi lain juga meningkatkan ancaman siber yang berdampak pada perilaku dan karakter generasi muda, seperti cyberbullying, phishing, pencurian identitas digital, penyebaran hoaks, dan pelanggaran privasi. Kondisi tersebut menunjukkan bahwa penguatan keamanan siber tidak cukup dilakukan melalui pendekatan teknologi, tetapi juga memerlukan penguatan pendidikan karakter dan kompetensi digital citizenship. Penelitian ini bertujuan untuk menganalisis ancaman siber yang dihadapi generasi muda serta mengkaji urgensi pendidikan karakter melalui perspektif digital citizenship dalam membangun warga negara digital yang berintegritas. Penelitian menggunakan pendekatan kualitatif dengan metode studi pustaka (library research) melalui analisis berbagai artikel ilmiah, buku, dan dokumen resmi internasional yang relevan. Analisis data dilakukan menggunakan model interaktif Miles, Huberman, dan Saldaña yang meliputi pengumpulan data, kondensasi data, penyajian data, serta penarikan kesimpulan. Hasil penelitian menunjukkan bahwa pendidikan karakter yang diintegrasikan dengan kompetensi digital citizenship berperan penting dalam meningkatkan kesadaran keamanan digital, etika bermedia, kemampuan berpikir kritis, serta perilaku digital yang bertanggung jawab. Penelitian ini menghasilkan model konseptual Ancaman Siber, Pendidikan Karakter, Kompetensi Digital Citizenship, dan Warga Negara Digital Berintegritas sebagai strategi penguatan Pendidikan Kewarganegaraan di era digital.

Kata kunci: Ancaman Siber, Pendidikan Karakter, Digital Citizenship, Warga Negara Digital, Pendidikan Kewarganegaraan.

Abstract

While digital transformation has provided numerous benefits to society, it has also increased cyber threats that impact the behavior and character of the younger generation, such as cyberbullying, phishing, digital identity theft, the spread of hoaxes, and privacy violations. This situation indicates that strengthening cybersecurity is not solely achieved through a technological approach, but also requires strengthening character education and digital citizenship competencies. This study aims to analyze the cyber threats faced by the younger generation and examine the urgency of character education through a digital citizenship perspective in developing digital citizens with integrity. The study used a qualitative approach with a library research method through the analysis of various relevant scientific articles, books, and official international documents. Data analysis was conducted using the interactive model of Miles, Huberman, and Saldaña, which includes data collection, data condensation, data presentation, and drawing conclusions. The results show that character education integrated with digital citizenship competencies plays a significant role in increasing digital security awareness, media ethics, critical thinking skills, and responsible digital behavior. This research produces a conceptual model of Cyber Threats, Character Education, Digital Citizenship Competence, and Digital Citizens with Integrity as a strategy to strengthen Citizenship Education in the digital era.

Keywords:

Cyber Threats, Character Education, Digital Citizenship, Digital Citizens, Civic Education.

PENDAHULUAN

Transformasi digital telah mengubah hampir seluruh aspek kehidupan masyarakat, termasuk dalam bidang pendidikan, ekonomi, komunikasi, pemerintahan, dan partisipasi kewarganegaraan. Pemanfaatan internet, media sosial, kecerdasan buatan (Artificial Intelligence), komputasi awan (cloud computing), serta berbagai platform digital telah menciptakan ruang interaksi baru yang tidak lagi dibatasi oleh ruang dan waktu. Perubahan tersebut menjadikan generasi muda sebagai kelompok yang paling aktif memanfaatkan teknologi digital karena mereka merupakan digital native yang lahir dan tumbuh di tengah perkembangan teknologi informasi. Di Indonesia, penetrasi internet terus mengalami peningkatan.

Survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2024 menunjukkan bahwa jumlah pengguna internet telah mencapai 221,56 juta jiwa atau sekitar 79,5% dari total penduduk Indonesia. Kondisi ini menunjukkan bahwa ruang digital telah menjadi bagian yang tidak terpisahkan dari kehidupan generasi muda, baik dalam proses pembelajaran, komunikasi, aktivitas ekonomi, maupun partisipasi sosial dan politik. Di balik berbagai manfaat tersebut, transformasi digital juga menghadirkan tantangan baru berupa meningkatnya ancaman siber. Ancaman tersebut tidak hanya berbentuk serangan terhadap sistem informasi, tetapi juga mencakup berbagai bentuk penyimpangan perilaku di ruang digital seperti cyberbullying, pencurian identitas (identity theft), phishing, penyebaran hoaks (misinformation dan disinformation), eksploitasi data pribadi, ujaran kebencian, hingga radikalisme digital. Berbagai ancaman tersebut menunjukkan bahwa ruang siber telah berkembang menjadi ruang sosial baru yang membutuhkan kemampuan literasi digital, etika digital, dan kesadaran keamanan digital yang memadai. Tanpa kompetensi tersebut, generasi muda berpotensi menjadi korban maupun pelaku berbagai bentuk kejahatan siber. Penelitian mengenai pendidikan kewarganegaraan digital juga menegaskan bahwa meningkatnya risiko seperti cyberbullying, agresi daring, dan pelanggaran privasi menuntut adanya pendidikan yang secara sistematis membangun perilaku digital yang aman dan bertanggung jawab.

Salah satu bentuk ancaman siber yang paling banyak dialami generasi muda adalah cyberbullying. Perkembangan media sosial telah memperluas ruang terjadinya intimidasi, penghinaan, pelecehan, maupun kekerasan verbal yang dilakukan melalui platform digital. Dampak cyberbullying tidak hanya memengaruhi kesehatan mental korban, tetapi juga dapat menurunkan kepercayaan diri, prestasi belajar, serta kualitas hubungan sosial. Penelitian terbaru menunjukkan bahwa penguatan kompetensi digital citizenship berpengaruh terhadap penurunan perilaku cyberbullying dan mendorong perilaku daring yang lebih bertanggung jawab. Dengan demikian, penguatan kewarganegaraan digital menjadi salah satu strategi penting dalam membangun lingkungan digital yang aman bagi peserta didik.

Dalam perspektif Pendidikan Kewarganegaraan, berbagai ancaman tersebut menunjukkan bahwa pendidikan karakter tidak lagi cukup diarahkan pada kehidupan sosial

di dunia nyata, tetapi juga harus mencakup perilaku warga negara dalam ruang digital. Pendidikan karakter pada era digital menuntut penguatan nilai-nilai integritas, tanggung jawab, empati, disiplin, berpikir kritis, dan etika digital agar generasi muda mampu memanfaatkan teknologi secara bertanggung jawab. Konsep digital citizenship menjadi pendekatan yang relevan karena mengintegrasikan literasi digital, etika digital, hak dan kewajiban warga negara digital, keamanan siber, serta partisipasi demokratis dalam lingkungan digital. Guru dan lembaga pendidikan memiliki peran penting dalam membangun kompetensi tersebut melalui proses pembelajaran yang sistematis dan kontekstual.

Sejumlah penelitian empiris menunjukkan bahwa pendidikan digital citizenship memiliki pengaruh positif terhadap pembentukan perilaku digital yang bertanggung jawab. Penelitian oleh Yuniawati et al. (2025) menemukan bahwa penerapan pendidikan digital citizenship berpengaruh signifikan terhadap penurunan perilaku cyberbullying pada siswa sekolah menengah. Penelitian tersebut menegaskan bahwa integrasi pendidikan digital citizenship dalam kurikulum mampu meningkatkan tanggung jawab, etika digital, dan perilaku daring yang positif sehingga dapat meminimalkan perilaku negatif di ruang siber. Demikian pula, Harrison dan Polizzi (2022) menjelaskan bahwa pendidikan digital citizenship yang didasarkan pada teori moral membantu remaja mengembangkan kemampuan mengambil keputusan etis ketika menghadapi situasi seperti cyberbullying, ujaran kebencian, maupun bentuk ketidaksantunan (incivility) di media sosial.

Berdasarkan kajian tersebut, masih terdapat kesenjangan penelitian (research gap), yaitu belum banyak penelitian yang mengintegrasikan ancaman siber, pendidikan karakter, dan digital citizenship dalam kerangka Pendidikan Kewarganegaraan. Padahal, ketiga aspek tersebut saling berkaitan dalam membentuk warga negara digital yang mampu menggunakan teknologi secara aman, etis, bertanggung jawab, dan berintegritas. Oleh karena itu, penelitian ini bertujuan untuk menganalisis ancaman siber yang dihadapi generasi muda serta mengkaji urgensi pendidikan karakter melalui perspektif digital citizenship sebagai strategi membangun warga negara digital yang berintegritas.

TINJAUAN PUSTAKA

Ancaman Siber

Transformasi digital telah membawa perubahan yang signifikan terhadap berbagai aspek kehidupan masyarakat, namun di sisi lain juga meningkatkan berbagai ancaman siber (cyber threats). Menurut National Institute of Standards and Technology (NIST, 2024), keamanan siber merupakan upaya untuk mengelola dan mengurangi risiko terhadap sistem informasi, aset digital, dan data melalui serangkaian proses tata kelola (governance), identifikasi (identify), perlindungan (protect), deteksi (detect), respons (respond), dan pemulihan (recover). Dalam kerangka tersebut, ancaman siber dipahami sebagai berbagai tindakan yang dapat mengganggu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi maupun sistem informasi sehingga berpotensi menimbulkan kerugian bagi individu, organisasi, maupun negara. Kerangka NIST Cybersecurity Framework (CSF) 2.0 juga menekankan bahwa keamanan siber tidak hanya

menjadi tanggung jawab sektor teknologi informasi, tetapi merupakan tanggung jawab seluruh organisasi melalui pendekatan manajemen risiko yang terintegrasi.

Seiring dengan meningkatnya penggunaan internet dan teknologi digital, bentuk ancaman siber juga mengalami perkembangan yang semakin kompleks. European Union Agency for Cybersecurity (ENISA, 2024) mengidentifikasi sejumlah ancaman siber utama yang saat ini paling banyak terjadi di berbagai sektor, yaitu malware, ransomware, phishing, rekayasa sosial (social engineering), pencurian identitas (identity theft), kebocoran data (data breaches), serangan terhadap rantai pasok (supply chain attacks), penyebaran disinformasi, serta eksploitasi kerentanan sistem informasi. Dalam konteks pendidikan, ancaman tersebut juga berkembang dalam bentuk cyberbullying, penyebaran hoaks, ujaran kebencian (hate speech), dan pelanggaran privasi yang banyak menasar peserta didik sebagai kelompok pengguna internet dengan intensitas tinggi. Kondisi tersebut menunjukkan bahwa ancaman siber tidak lagi hanya berupa serangan teknis terhadap perangkat dan jaringan, tetapi juga telah berkembang menjadi persoalan sosial yang memengaruhi keamanan, kesehatan mental, serta kualitas interaksi masyarakat di ruang digital.

Laporan International Telecommunication Union (ITU) melalui Global Cybersecurity Index 2024 menunjukkan bahwa ancaman siber telah menjadi tantangan global yang memerlukan kesiapan setiap negara dalam aspek hukum, teknis, organisasi, peningkatan kapasitas sumber daya manusia, dan kerja sama internasional. ITU menegaskan bahwa peningkatan kapasitas (capacity building) melalui pendidikan dan literasi keamanan siber merupakan salah satu pilar utama dalam memperkuat ketahanan siber masyarakat. Oleh karena itu, sektor pendidikan memiliki peran strategis dalam membangun kesadaran keamanan siber (cybersecurity awareness) sejak dini agar generasi muda mampu mengenali, mencegah, dan merespons berbagai bentuk ancaman digital secara tepat.

Dalam perspektif Pendidikan Kewarganegaraan, ancaman siber tidak hanya dipandang sebagai persoalan keamanan teknologi, tetapi juga sebagai persoalan kewarganegaraan digital (digital citizenship) karena berkaitan dengan hak digital, kewajiban, keamanan, tanggung jawab, serta partisipasi warga negara dalam ruang digital. Oleh sebab itu, penyelesaian berbagai ancaman siber tidak cukup dilakukan melalui pendekatan teknologi semata, tetapi juga memerlukan pendekatan pendidikan yang berorientasi pada pembentukan karakter, penguatan literasi digital, dan pengembangan kompetensi kewarganegaraan digital agar generasi muda mampu menggunakan teknologi secara aman, etis, bertanggung jawab, dan berintegritas.

Pendidikan Karakter

Pendidikan karakter merupakan proses pendidikan yang bertujuan mengembangkan nilai-nilai moral, etika, tanggung jawab, empati, integritas, dan kepedulian sosial agar peserta didik mampu mengambil keputusan yang bertanggung jawab dalam kehidupan pribadi maupun bermasyarakat. Dalam konteks pendidikan abad ke-21, pendidikan karakter tidak hanya berorientasi pada pembentukan perilaku individu, tetapi juga pada pengembangan kompetensi kewarganegaraan yang memungkinkan peserta didik berpartisipasi secara aktif dalam masyarakat yang demokratis dan berkelanjutan. OECD Learning Compass 2030 menegaskan bahwa pendidikan harus membentuk peserta didik sebagai

individu yang memiliki knowledge, skills, attitudes, dan values sehingga mampu menciptakan kesejahteraan individu maupun masyarakat melalui tindakan yang bertanggung jawab. Kompetensi tersebut meliputi kemampuan berpikir kritis, tanggung jawab, kolaborasi, empati, dan integritas sebagai fondasi pembelajaran sepanjang hayat.

Seiring berkembangnya transformasi digital, pendidikan karakter tidak lagi hanya diarahkan pada pembentukan perilaku di lingkungan nyata, tetapi juga harus mencakup perilaku individu dalam ruang digital. UNESCO (2024) melalui *Global Citizenship Education in a Digital Age: Teacher Guidelines* menegaskan bahwa pendidikan karakter pada era digital harus membekali peserta didik dengan pengetahuan, keterampilan, nilai, dan sikap untuk berinteraksi secara etis, bertanggung jawab, inklusif, serta mampu menghadapi tantangan seperti misinformasi, disinformasi, ujaran kebencian, dan kekerasan daring. Oleh karena itu, nilai-nilai seperti kejujuran, tanggung jawab, penghormatan terhadap hak orang lain, etika komunikasi, dan kepedulian sosial menjadi fondasi utama dalam mencegah penyalahgunaan teknologi, penyebaran hoaks, maupun cyberbullying.

Dalam perspektif Pendidikan Kewarganegaraan, pendidikan karakter memiliki fungsi strategis dalam membentuk warga negara yang demokratis, berintegritas, serta mampu menggunakan teknologi secara bertanggung jawab. Mulyono (2021) menjelaskan bahwa pembentukan karakter merupakan prasyarat utama dalam membangun kompetensi kewarganegaraan digital (*digital citizenship competence*) karena karakter menjadi dasar bagi penggunaan teknologi yang etis, bertanggung jawab, serta selaras dengan nilai-nilai demokrasi dan Pancasila. Dengan demikian, pendidikan karakter berfungsi sebagai fondasi moral yang mendukung terbentuknya warga negara digital yang bertanggung jawab.

Kompetensi *Digital Citizenship*

Konsep *Digital Citizenship* pertama kali dikembangkan secara sistematis oleh Mike Ribble, yang mendefinisikannya sebagai norma penggunaan teknologi yang tepat, bertanggung jawab, dan memberdayakan (*appropriate, responsible, and empowered technology use*). Model Ribble menempatkan *digital citizenship* sebagai seperangkat kompetensi yang diperlukan individu untuk menggunakan teknologi secara aman, etis, produktif, dan bertanggung jawab. Model tersebut terdiri atas sembilan elemen utama, yaitu *digital access*, *digital commerce*, *digital communication and collaboration*, *digital etiquette*, *digital literacy*, *digital health and wellness*, *digital law*, *digital rights and responsibilities*, serta *digital security and privacy*.

Perkembangan kajian mutakhir menunjukkan bahwa konsep *digital citizenship* tidak lagi dipahami sekadar sebagai perilaku menggunakan teknologi secara aman, tetapi juga sebagai kompetensi kewargaan yang mencakup dimensi sosial, etika, demokrasi, dan partisipasi publik. Choi (2016; 2018) mengembangkan konsep *digital citizenship* melalui empat dimensi utama, yaitu etika digital (*digital ethics*), literasi digital, keterlibatan kewargaan (*civic engagement*), dan kemampuan berpikir kritis terhadap informasi digital. Menurut Choi, warga negara digital bukan hanya pengguna teknologi, melainkan individu yang mampu menggunakan media digital untuk berpartisipasi dalam kehidupan demokrasi secara kritis, bertanggung jawab, dan berorientasi pada kepentingan publik.

Pandangan tersebut diperkuat oleh Webster (2025) yang mendefinisikan digital citizenship sebagai kemampuan individu untuk menggunakan teknologi secara sadar (considered use), membangun kepedulian terhadap komunitas (community care), serta melakukan tindakan kewargaan (civic action) dalam masyarakat digital. Definisi ini memperluas konsep digital citizenship dari sekadar keamanan digital menuju pembentukan warga negara yang aktif, kritis, dan beretika dalam ruang digital.

Selanjutnya, International Society for Technology in Education (ISTE, 2024) menegaskan bahwa kompetensi digital citizenship mencakup kemampuan peserta didik untuk mengenali peluang dan risiko teknologi, menjaga keamanan serta privasi digital, menghormati hak digital orang lain, berkomunikasi secara etis, serta menggunakan teknologi untuk meningkatkan kesejahteraan individu maupun masyarakat. Sementara itu, European Commission melalui kerangka DigComp 2.2 menempatkan digital citizenship sebagai bagian dari kompetensi digital yang meliputi literasi informasi dan data, komunikasi dan kolaborasi, penciptaan konten digital, keamanan digital (digital safety), serta pemecahan masalah (problem solving).

Berdasarkan berbagai konsep tersebut, penelitian ini memandang kompetensi digital citizenship sebagai kemampuan individu untuk menggunakan teknologi secara aman, menjaga keamanan data pribadi, menghormati hak digital orang lain, berpikir kritis terhadap informasi digital, menerapkan etika komunikasi digital, serta berpartisipasi secara aktif dalam kehidupan demokrasi melalui media digital. Berbagai penelitian Scopus terbaru juga menunjukkan bahwa penguatan pendidikan digital citizenship mampu meningkatkan perilaku digital yang bertanggung jawab sekaligus menurunkan perilaku cyberbullying, misinformasi, dan agresi daring melalui penguatan empati, tanggung jawab, dan kesadaran etis peserta didik.

Warga Negara Digital Berintegritas

Perkembangan teknologi digital telah melahirkan konsep warga negara digital (digital citizen), yaitu individu yang tidak hanya memiliki kemampuan menggunakan teknologi digital, tetapi juga memahami hak, kewajiban, etika, tanggung jawab, dan partisipasi sebagai warga negara dalam masyarakat digital. Menurut Webster (2025), warga negara digital merupakan individu yang mampu memanfaatkan teknologi secara sadar, peduli terhadap komunitas digital, dan berkontribusi secara aktif dalam kehidupan demokrasi melalui tindakan kewargaan yang bertanggung jawab.

Dalam perspektif Pendidikan Kewarganegaraan, warga negara digital yang berintegritas adalah individu yang mampu mengintegrasikan kompetensi digital dengan nilai-nilai karakter seperti integritas, tanggung jawab, kejujuran, toleransi, dan kepedulian sosial. UNESCO (2024) menegaskan bahwa tujuan pendidikan kewargaan global di era digital adalah membentuk peserta didik yang mampu bertindak secara etis, bertanggung jawab, inklusif, serta menghormati hak asasi manusia baik di lingkungan fisik maupun digital.

Karakteristik warga negara digital yang berintegritas meliputi kemampuan menjaga keamanan data pribadi, menghormati hak digital orang lain, menolak penyebaran hoaks dan ujaran kebencian, menerapkan etika komunikasi digital, berpikir kritis terhadap informasi,

serta berpartisipasi aktif dalam kehidupan demokrasi digital. Oleh karena itu, pembentukan warga negara digital yang berintegritas tidak hanya bergantung pada penguasaan teknologi, tetapi juga pada keberhasilan pendidikan karakter yang diinternalisasikan melalui pengembangan kompetensi digital citizenship. Model ini menunjukkan bahwa pendidikan karakter berfungsi sebagai fondasi moral, sedangkan digital citizenship menjadi kompetensi operasional yang memungkinkan nilai-nilai tersebut diwujudkan dalam perilaku nyata di ruang digital.

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi pustaka (library research). Pendekatan ini dipilih karena bertujuan untuk menganalisis secara komprehensif keterkaitan antara ancaman siber, pendidikan karakter, kompetensi digital citizenship, dan pembentukan warga negara digital yang berintegritas berdasarkan berbagai hasil penelitian dan dokumen ilmiah yang relevan. Studi pustaka memungkinkan peneliti melakukan sintesis konsep, teori, dan temuan empiris sehingga diperoleh model konseptual yang dapat menjelaskan hubungan antarvariabel dalam konteks Pendidikan Kewarganegaraan.

Sumber data penelitian terdiri atas sumber primer dan sumber sekunder. Sumber primer meliputi artikel jurnal nasional terakreditasi dan jurnal internasional bereputasi yang diterbitkan pada rentang tahun 2020–2025, khususnya yang membahas keamanan siber (cybersecurity), pendidikan karakter (character education), digital citizenship, dan Pendidikan Kewarganegaraan. Selain itu, penelitian ini juga menggunakan dokumen resmi dari National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (2024), International Telecommunication Union (ITU) Global Cybersecurity Index (2024), European Union Agency for Cybersecurity (ENISA) Threat Landscape (2024), UNESCO Global Citizenship Education in a Digital Age (2024), OECD Learning Compass 2030, ISTE Digital Citizenship Framework (2024), serta European Commission DigComp 2.2. Adapun sumber sekunder berupa buku, prosiding, laporan penelitian, dan dokumen pendukung lainnya yang memiliki relevansi dengan fokus penelitian.

Pengumpulan data dilakukan melalui teknik dokumentasi, yaitu mengidentifikasi, menyeleksi, mengorganisasi, dan mengkaji berbagai literatur sesuai tema penelitian. Kriteria inklusi sumber meliputi: (1) memiliki keterkaitan dengan ancaman siber, pendidikan karakter, atau digital citizenship; (2) dipublikasikan oleh lembaga resmi atau jurnal ilmiah bereputasi; dan (3) memuat temuan empiris atau konseptual yang mendukung analisis penelitian.

Analisis data menggunakan model analisis interaktif yang dikembangkan oleh Miles, Huberman, dan Saldaña (2014) yang meliputi empat tahapan, yaitu pengumpulan data (data collection), kondensasi data (data condensation), penyajian data (data display), dan penarikan serta verifikasi kesimpulan (conclusion drawing/verification). Pada tahap kondensasi data, peneliti mengelompokkan berbagai konsep ke dalam empat tema utama, yaitu ancaman siber, pendidikan karakter, kompetensi digital citizenship, dan warga negara digital berintegritas. Selanjutnya dilakukan analisis sintesis untuk membangun hubungan

konseptual antartema sehingga diperoleh model penguatan karakter berbasis digital citizenship dalam menghadapi ancaman siber.

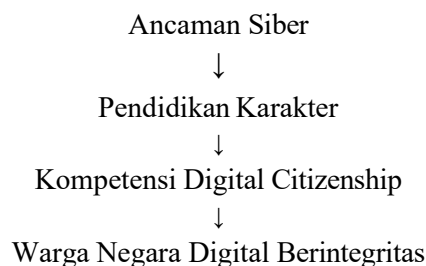
Untuk menjaga kredibilitas hasil penelitian, dilakukan triangulasi sumber, yaitu membandingkan informasi dari berbagai jurnal ilmiah, dokumen kebijakan internasional, dan hasil penelitian terdahulu. Teknik ini bertujuan untuk meningkatkan validitas interpretasi serta mengurangi potensi bias dalam penyusunan model konseptual penelitian.

HASIL DAN PEMBAHASAN

Hasil kajian pustaka menunjukkan bahwa ancaman siber terhadap generasi muda semakin kompleks seiring meningkatnya penggunaan teknologi digital. Berdasarkan NIST Cybersecurity Framework 2.0 (2024), ENISA Threat Landscape (2024), dan ITU Global Cybersecurity Index (2024), ancaman yang paling dominan meliputi *cyberbullying*, *phishing*, pencurian identitas digital, penyebaran hoaks, kebocoran data pribadi, serta ujaran kebencian di ruang digital. Ancaman tersebut tidak hanya berdampak pada aspek keamanan informasi, tetapi juga memengaruhi perkembangan karakter, perilaku sosial, dan partisipasi kewarganegaraan generasi muda.

Hasil sintesis berbagai penelitian juga menunjukkan bahwa pendidikan karakter memiliki peran penting dalam membangun perilaku digital yang bertanggung jawab. Nilai-nilai seperti integritas, tanggung jawab, kejujuran, empati, dan disiplin menjadi landasan bagi peserta didik dalam menggunakan teknologi secara etis. Penguatan pendidikan karakter yang diintegrasikan dengan kompetensi *digital citizenship* terbukti mampu meningkatkan kesadaran keamanan digital, etika bermedia, kemampuan berpikir kritis terhadap informasi, serta menekan perilaku negatif seperti *cyberbullying* dan penyebaran disinformasi.

Berdasarkan hasil kajian tersebut, penelitian ini merumuskan sebuah model konseptual yang menggambarkan hubungan antara ancaman siber, pendidikan karakter, kompetensi *digital citizenship*, dan pembentukan warga negara digital yang berintegritas sebagaimana ditunjukkan pada Gambar 1.



Gambar 1. Model Konseptual Penelitian

Model tersebut menunjukkan bahwa pendidikan karakter berfungsi sebagai fondasi dalam membentuk kompetensi *digital citizenship*, yang selanjutnya berkontribusi pada terbentuknya warga negara digital yang mampu menggunakan teknologi secara aman, etis, bertanggung jawab, dan berintegritas.

Hasil kajian menunjukkan bahwa ancaman siber telah berkembang menjadi tantangan yang tidak hanya berkaitan dengan keamanan teknologi, tetapi juga berdampak

pada perilaku sosial dan karakter generasi muda. Berdasarkan NIST Cybersecurity Framework 2.0 (2024) dan ENISA Threat Landscape (2024), ancaman seperti *phishing*, *cyberbullying*, kebocoran data pribadi, dan penyebaran disinformasi merupakan risiko utama yang dihadapi pengguna internet. Sementara itu, ITU Global Cybersecurity Index (2024) menegaskan bahwa penguatan kapasitas sumber daya manusia melalui pendidikan menjadi strategi penting dalam meningkatkan ketahanan siber suatu negara.

Temuan penelitian menunjukkan bahwa pendidikan karakter memiliki peran strategis dalam membentuk perilaku digital yang bertanggung jawab. Nilai-nilai seperti integritas, kejujuran, tanggung jawab, dan empati menjadi dasar bagi generasi muda untuk menggunakan teknologi secara etis serta menghindari perilaku negatif seperti penyebaran hoaks dan *cyberbullying*. Hal ini sejalan dengan UNESCO (2024) yang menekankan pentingnya penguatan nilai, sikap, dan tanggung jawab dalam membentuk warga global dan warga digital yang bertanggung jawab.

Selain pendidikan karakter, kompetensi *digital citizenship* menjadi faktor penting dalam menghadapi ancaman siber. Menurut ISTE (2024) dan European Commission melalui DigComp 2.2, kompetensi tersebut meliputi kemampuan menggunakan teknologi secara aman, menjaga privasi, menghormati hak digital orang lain, berpikir kritis terhadap informasi, serta berpartisipasi secara positif di ruang digital. Pendapat ini diperkuat oleh Webster (2025) yang menyatakan bahwa *digital citizenship* merupakan kemampuan menggunakan teknologi secara bertanggung jawab sekaligus berpartisipasi aktif dalam kehidupan masyarakat digital.

Berdasarkan hasil sintesis berbagai literatur, penelitian ini menghasilkan model konseptual Ancaman Siber → Pendidikan Karakter → Kompetensi Digital Citizenship → Warga Negara Digital Berintegritas. Model tersebut menunjukkan bahwa pendidikan karakter menjadi fondasi moral, sedangkan kompetensi *digital citizenship* berfungsi sebagai implementasi nilai-nilai karakter dalam kehidupan digital. Dengan demikian, pembentukan warga negara digital yang berintegritas tidak hanya bergantung pada penguasaan teknologi, tetapi juga pada keberhasilan pendidikan karakter yang diintegrasikan dengan kompetensi *digital citizenship* dalam pembelajaran Pendidikan Kewarganegaraan.

KESIMPULAN

Penelitian ini menunjukkan bahwa ancaman siber telah berkembang menjadi tantangan multidimensional yang tidak hanya mengancam keamanan sistem informasi, tetapi juga memengaruhi perilaku, karakter, dan kualitas partisipasi generasi muda di ruang digital. Berbagai bentuk ancaman seperti *cyberbullying*, *phishing*, pencurian identitas digital, penyebaran hoaks, dan pelanggaran privasi menuntut adanya upaya preventif yang tidak hanya berfokus pada aspek teknologi, tetapi juga pada aspek pendidikan.

Hasil kajian menegaskan bahwa pendidikan karakter memiliki peran strategis sebagai fondasi moral dalam membentuk perilaku digital yang bertanggung jawab. Nilai-nilai integritas, tanggung jawab, kejujuran, empati, dan etika menjadi dasar bagi generasi muda dalam memanfaatkan teknologi secara bijaksana. Nilai-nilai tersebut perlu diperkuat melalui pengembangan kompetensi *digital citizenship* yang mencakup literasi digital, etika digital,

keamanan digital, kemampuan berpikir kritis, serta partisipasi aktif dalam kehidupan demokrasi di ruang digital.

Berdasarkan sintesis berbagai literatur, penelitian ini menawarkan model konseptual Ancaman Siber → Pendidikan Karakter → Kompetensi Digital Citizenship → Warga Negara Digital Berintegritas. Model ini menunjukkan bahwa pembentukan warga negara digital yang berintegritas tidak cukup hanya melalui peningkatan kemampuan teknis dalam menggunakan teknologi, tetapi harus didukung oleh internalisasi nilai-nilai karakter dan penguatan kompetensi kewarganegaraan digital secara terpadu.

Implikasi penelitian ini menegaskan bahwa Pendidikan Kewarganegaraan perlu mengintegrasikan pendidikan karakter, literasi digital, dan digital citizenship ke dalam proses pembelajaran sebagai strategi untuk mempersiapkan generasi muda yang mampu menghadapi ancaman siber sekaligus berpartisipasi secara etis, kritis, dan bertanggung jawab dalam masyarakat digital.

Meskipun penelitian ini memberikan kontribusi berupa model konseptual penguatan karakter berbasis digital citizenship, penelitian ini masih bersifat konseptual melalui pendekatan studi pustaka. Oleh karena itu, penelitian selanjutnya disarankan melakukan pengujian empiris terhadap model yang diusulkan melalui pendekatan kuantitatif, kualitatif, maupun mixed methods pada berbagai jenjang pendidikan sehingga efektivitas model dalam membentuk warga negara digital yang berintegritas dapat dibuktikan secara lebih komprehensif.

DAFTAR PUSTAKA

- Asosiasi Penyelenggara Jasa Internet Indonesia. (2024). *Survei penetrasi internet Indonesia 2024*. <https://apjii.or.id>
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). Sage Publications.
- Ribble, M. (2015). *Digital citizenship in schools* (3rd ed.). International Society for Technology in Education.
- Choi, M. (2016). A concept analysis of digital citizenship for democratic citizenship education in the Internet age. *Theory & Research in Social Education*, 44(4), 565–607. <https://doi.org/10.1080/00933104.2016.1210549>
- Choi, M. (2018). Development of a scale to measure digital citizenship among young adults. *Computers & Education*, 123, 54–65. <https://doi.org/10.1016/j.compedu.2018.04.006>
- European Commission, Joint Research Centre. (2022). *The Digital Competence Framework for Citizens (DigComp 2.2): With new examples of knowledge, skills and attitudes*. Publications Office of the European Union.
- European Union Agency for Cybersecurity. (2024). *ENISA Threat Landscape 2024*. ENISA.
- International Telecommunication Union. (2024). *Global Cybersecurity Index 2024*.
- ITU. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce.

- Harrison, T., & Polizzi, G. (2022). Developing digital citizenship through moral education in the digital age. *Education and Information Technologies*, 27(3), 4175–4197. <https://doi.org/10.1007/s10639-021-10781-9>
- Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2023). Cyber security in the education sector: A systematic literature review. *Computers & Security* 127, 103126. <https://doi.org/10.1016/j.cose.2023.103126>
- Mulyono, B. (2021). Digital citizenship competence: Initiating ethical citizenship in the digital era. *Jurnal Civics: Media Kajian Kewarganegaraan*, 18(1), 1–15.
- OECD. (2020). *OECD Learning Compass 2030*. OECD Publishing.
- UNESCO. (2024). *Global Citizenship Education in a Digital Age: Teacher Guidelines*. UNESCO.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Webster, J. (2025). Defining digital citizenship and digital citizenship education: A Delphi study. *Journal of Research on Technology in Education*. Advance online publication. <https://doi.org/10.1080/15391523.2025.2536564>
- Yuniawati, E. I., et al. (2025). Digital citizenship, learning outcomes, and negative online cyberbullying behavior among junior high school students. *International Journal of Advances in Social Sciences and Humanities*.