JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i1.8336

EDUKASI MASYARAKAT TENTANG KEAMANAN SIBER DALAM TANTANGAN DAN SOLUSI DI ERA DIGITAL

Rama Wijaya[1*], Didi Juardi[2]

[1,2]universitas Singaperbangsa Karawang, Jl.HS.Ronggo Waluyo, Puseurjaya, Telukjambe Timur, Karawang, Jawa Barat 41361, Telp. (0267) 641177

Keywords:
Keamanan Siber; Literasi Digital; Edukasi; *Low-Tech*; Inklusivitas.

Corespondent Email:
2110631170095@student.unsika.ac.id

Abstrak. Kemajuan teknologi digital telah memberikan kemudahan dalam berbagai aspek kehidupan, namun juga meningkatkan ancaman terhadap keamanan siber. Penelitian ini bertujuan untuk menganalisis tantangan utama dalam edukasi keamanan siber di Indonesia serta menawarkan solusi inklusif dan adaptif bagi masyarakat dengan tingkat literasi digital yang beragam. Metode yang digunakan adalah kualitatif dengan pendekatan studi dokumen terhadap laporan pemerintah, survei nasional, artikel ilmiah, dan berita daring. Hasil penelitian menunjukkan bahwa rendahnya kesadaran masyarakat, kesenjangan akses digital, serta belum optimalnya koordinasi kebijakan menjadi hambatan utama dalam mewujudkan keamanan siber nasional. Pendekatan edukatif berbasis komunitas dan penggunaan media *low-tech* seperti pamflet dan pelatihan langsung terbukti efektif meningkatkan literasi digital hingga 60% di daerah dengan infrastruktur terbatas. Penelitian ini merekomendasikan tiga langkah strategis, yaitu peningkatan literasi digital inklusif, pembentukan lembaga pengawas data pribadi independen, serta kolaborasi lintas sektor untuk memperkuat ketahanan siber nasional.

Abstract. *The advancement of digital technology has brought convenience to many aspects of life but also increased cybersecurity threats. This study aims to analyze the main challenges in cybersecurity education in Indonesia and propose inclusive and adaptive solutions for communities with diverse levels of digital literacy. A qualitative research method with document analysis was employed, using data from government reports, national surveys, academic articles, and online news. The findings reveal that low public awareness, digital access inequality, and suboptimal policy coordination are the main obstacles to achieving national cybersecurity resilience. Community-based education and low-tech media such as pamphlets and direct training have proven effective in improving digital literacy by up to 60% in low-infrastructure areas. The study recommends three strategic actions: enhancing inclusive digital literacy, establishing an independent data protection authority, and fostering cross-sector collaboration to strengthen national cybersecurity resilience.*

1. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi telah mengubah cara masyarakat berinteraksi, bekerja, dan belajar [1]. Di era digital ini, perangkat digital yang terhubung ke internet menjadi bagian penting dari kehidupan sehari – hari [2]. Namun, semakin tingginya adopsi teknologi juga membuka celah bagi

ancaman siber seperti pencurian data, *phising, malware,* dan *ransomware* [3]. Hal ini menunjukkan bahwa literasi digital, khususnya dalam aspek keamanan siber, menjadi kebutuhan yang mendesak untuk memastikan masyarakat mampu melindungi diri dari risiko di dunia maya [4]. Selain meningkatnya ancaman seperti pencurian data, *phishing*, dan *malware*, dinamika di media sosial juga memperkuat munculnya berbagai bentuk ancaman siber. Platform seperti *Twitter* sering digunakan masyarakat untuk mengekspresikan opini, kritik, atau bahkan ujaran kebencian yang berpotensi menimbulkan konflik sosial dan mengganggu keamanan digital. Kondisi ini menunjukkan bahwa ancaman siber tidak hanya bersumber dari aktivitas teknis semata, tetapi juga dari perilaku komunikasi digital masyarakat. Oleh karena itu, diperlukan upaya yang tidak hanya bersifat teknis melalui sistem deteksi otomatis, tetapi juga edukatif untuk meningkatkan kesadaran dan literasi keamanan siber di berbagai lapisan masyarakat [5].

Penelitian sebelumnya menunjukkan berbagai upaya telah dilakukan untuk meningkatkan literasi digital dalam hal keamanan siber. Misalnya, [6] meneliti efektivitas pelatihan literasi digital pada siswa SMA berbasis teknologi, yang menunjukkan peningkatan pemahaman yang signifikan dalam kemampuan siswa terhadap konsep dasar teknologi informasi dan keamanan digital. Studi [7] meneliti strategi membangun kebudayaan keamanan siber yang berkelanjutan, yang berhasil meningkatkan kesadaran etika keamanan siber melalui pendekatan pendidikan, gamifikasi, dan pengembangan *chatbot*. Selain itu, penelitian oleh [8] meneliti efektivitas model pembelajaran adaptif, yang menunjukkan bahwa pendekatan ini mampu meningkatkan konsentrasi siswa hingga menciptakan pengalaman belajar yang lebih personal, meskipun keterbatasan akses internet di beberapa daerah tetap menjadi tantangan signifikan.

Kesenjangan penelitian terletak pada kurangnya pendekatan edukasi keamanan siber yang dapat menjangkau seluruh lapisan masyarakat dengan latar belakang dan akses teknologi yang beragam. Banyak penelitian yang fokus pada konten edukasi, tetapi belum banyak yang mengembangkan strategi inovatif untuk meningkatkan aksesibilitas, terutama bagi kelompok dengan keterbatasan teknologi atau literasi digital. Selain itu, masih sedikit penelitian yang mengevaluasi efektivitas pendekatan berbasis komunitas atau teknologi rendah *(low-tech)* dalam meningkatkan kesadaran keamanan siber.

Penelitian ini bertujuan untuk menganalisis tantangan utama dalam edukasi keamanan siber di Indonesia, serta menawarkan solusi inovatif yang inklusif dan adaptif terhadap kebutuhan masyarakat. Pertanyaan utama penelitian adalah: (1) Apa saja hambatan yang dihadapi masyarakat dalam memahami dan menerapkan keamanan siber? (2) Bagaimana strategi yang efektif untuk mengatasi hambatan tersebut? Penelitian ini diharapkan memberikan kontribusi dalam mengembangkan pendekatan edukasi yang lebih inklusif dan efektif, sekaligus memperkuat literasi keamanan digital masyarakat Indonesia.

2. TINJAUAN PUSTAKA

Keamanan siber mencakup upaya melindungi sistem, jaringan, dan data dari ancaman digital seperti *malware, ransomware, phising*, dan pencurian data [9]. Menurut [10], aspek utama keamanan siber meliputi kerahasiaan, integritas, dan ketersediaan data. Dengan meningkatnya jumlah perangkat yang terhubung ke internet, tantangan dalam menjaga keamanan informasi juga semakin kompleks. Literasi keamanan siber yang memadai diperlukan untuk mengurangi risiko yang dihadapi pengguna individu dan institusi.

Literasi digital didefinisikan sebagai kemampuan menggunakan teknologi secara aman, etis, dan produktif [11]. Menurut [12], literasi digital mencakup dimensi teknis, kognitif, dan sosial, termasuk kesadaran akan ancaman siber. Penelitian oleh [13] menunjukkan bahwa program edukasi berbasis literasi digital mampu meningkatkan kesadaran individu terhadap potensi risiko online serta keterampilan mitigasinya.

Beberapa pendekatan yang digunakan dalam edukasi keamanan siber melibatkan pelatihan berbasis teknologi, gamifikasi, dan media interaktif. Penelitian [14] mengungkapkan bahwa pelatihan berbasis teknologi dapat memberikan pengalaman belajar yang mendalam, meskipun aksesibilitas menjadi tantangan. Gamifikasi, seperti diterapkan oleh [15], terbukti efektif dalam meningkatkan

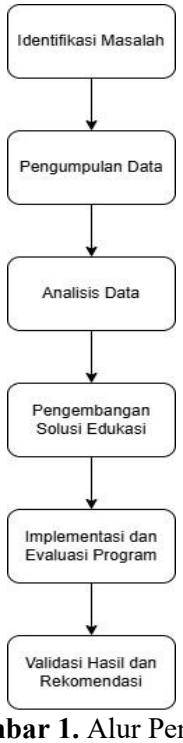
motivasi belajar, terutama pada generasi muda. Namun, pendekatan ini perlu disesuaikan untuk masyarakat dengan akses teknologi yang terbatas.

Strategi edukasi berbasis komunitas dianggap efektif untuk menjangkau kelompok masyarakat yang memiliki keterbatasan akses teknologi [16]. Selain itu, pendekatan *low-tech* seperti penggunaan media cetak dan penyuluhan langsung menjadi alternatif yang relevan untuk konteks masyarakat di daerah terpencil.

Literasi digital di Indonesia masih memiliki tantangan signifikan, terutama di daerah dengan akses internet terbatas [17]. Menurut laporan APJII (2022), kesenjangan digital antara wilayah perkotaan dan pedesaan memengaruhi tingkat pemahaman keamanan siber masyarakat. Penelitian oleh Prasetyo et al. (2021) merekomendasikan pendekatan berbasis komunitas yang memanfaatkan budaya lokal dan media sederhana untuk meningkatkan literasi digital [18].

3. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode kualiatif. Gambar 1 merupakan bagan alur penelitian.



Gambar 1. Alur Penelitian

3.1. Identifikasi Masalah

Tahap awal penelitian dilakukan dengan menelaah kondisi literasi digital dan keamanan siber di Indonesia melalui berbagai sumber seperti laporan Kominfo, data survei APJII, dan publikasi ilmiah. Proses ini bertujuan untuk mengidentifikasi permasalahan utama yang dihadapi masyarakat, antara lain rendahnya kesadaran terhadap ancaman siber, kesenjangan akses teknologi di wilayah tertentu, serta minimnya pendekatan edukasi yang inklusif dan mudah dijangkau.

3.2. Pengumpulan Data

Penelitian ini menggunakan metode studi dokumen untuk mengumpulkan data kualitatif. Sumber data diperoleh dari berbagai dokumen dan publikasi yang relevan, meliputi:

a. Laporan resmi pemerintah, seperti publikasi Kementrian Komunikasi dan Informatika (Kominfo) dan Badan Siber dan Sandi Negara (BSSN).
b. Laporan survei nasional, seperti hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mengenai tingkat penggunaan internet dan literasi digital masyarakat.
c. Berita daring dari media kredibel (Kompas, CNN Indonesia, Detik.com, dan lainnya) yang menyoroti fenomena aktual terkait ancaman dan kebijakan keamanan siber.

Dokumen yang terpilih kemudian dibaca secara menyeluruh, dipahami konteksnya, dan diklasifikasikan berdasarkan tema seperti tantangan keamanan siber, bentuk ancaman, kebijakan pemerintah, serta model edukasi yang digunakan di masyarakat.

3.3. Analisis Data

Data dianalisis dengan pendekatan analisis tematik kualitatif, mengikuti tahapan menurut [19] :

(1) *Skimming* (membaca cepat untuk memahami konteks umum)
(2) *Reading* (pemahaman mendalam)
(3) *Interpretation* (penafsiran isi dokumen)

Setiap informasi penting dari dokumen dikodekan dan dikelompokkan menjadi beberapa tema utama, seperti tantangan keamanan siber, strategi edukasi efektif, dan pendekatan inklusif berbasis komunitas. Hasil analisis kemudian dibandingkan untuk

menemukan pola dan hubungan antartema yang relevan dengan fokus penelitian.

3.4. Pengembangan Solusi Edukasi

Berdasarkan hasil analisis, peneliti merancang solusi edukasi keamanan siber yang bersifat inklusif dan mudah diterapkan. Solusi difokuskan pada edukasi berbasis komunitas dan penggunaan media *low-tech* seperti pamflet, poster, atau pelatihan langsung di masyarakat. Pendekatan ini dipilih agar informasi keamanan siber dapat menjangkau kelompok dengan keterbatasan akses internet maupun literasi digital.

3.5. Implementasi dan Evaluasi Program

Solusi yang dikembangkan diuji dalam bentuk percontohan pada beberapa komunitas lokal. Evaluasi dilakukan secara kualitatif melalui wawancara singkat dan umpan balik dari peserta pelatihan. Selain itu, dilakukan perbandingan antara pemahaman peserta sebelum dan sesudah pelatihan untuk menilai efektivitas edukasi berbasis komunitas dan media *low-tech* dalam meningkatkan kesadaran keamanan siber.

3.6. Validasi Hasil dan Rekomendasi

Tahap akhir penelitian dilakukan dengan memvalidasi hasil temuan dan mengevaluasi efektivitas solusi yang telah diterapkan. Beberapa hasil validasi, disusun rekomendasi praktis untuk pengembangan strategi edukasi keamanan siber yang lebih luas. Rekomendasi diarahkan kepada pemerintah, lembaga pendidikan, dan organisasi non-pemerintah untuk memperkuat literasi digital masyarakat secara inklusif dan berkelanjutan

4. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil dan pembahasan analisis tematik terhadap berbagai dokumen dan publikasi sebagaimana dijelaskan dalam metode penelitian.

Hasil

4.1. Identifikasi Masalah

Tahap awal penelitian dilakukan untuk menelaah kondisi literasi digital dan keamanan siber di Indonesia melalui laporan resmi, survei nasional, dan publikasi ilmiah. Hasil identifikasi menunjukkan tiga permasalahan utama:

(1) Rendahnya kesadaran keamanan siber masyarakat.
(2) Kesenjangan akses dan infrastruktur digital.
(3) Belum optimalnya implementasi kebijakan perlindungan data pribadi.

Berdasarkan laporan [20], tingkat partisipasi literasi digital masyarakat masih belum merata, meskipun Gerakan Nasional Literasi Digital (GNLD) Siberkreasi telah menjangkau lebih dari 20 juta orang. Sementara itu, [21] melaporkan bahwa penetrasi internet nasional baru mencapai 78,19%, dengan kesenjangan signifikan antara wilayah urban (87,55%) dan rural (79,79%). Kondisi tersebut diperparah oleh meningkatnya ancaman keamanan siber seperti *phising, malware*, dan data *breach*, yang menunjukkan lemahnya kesadaran serta perlindungan data di tingkat individu dan institusi.

4.2. Hasil Studi Dokumen

Penelitian ini menggunakan metode studi dokumen untuk menelaah laporan pemerintah, survei nasional, artikel ilmiah, dan berita kredibel. Hasil telaah menghasilkan beberapa temuan tematik utama sebagai berikut:

4.2.1. Kesenjangan Akses dan Infrastruktur Digital

Data APJII 2023 dan BPS 2024 menunjukkan bahwa wilayah dengan literasi tinggi seperti DKI Jakarta dan DI Yogyakarta memiliki kesiapan digital yang jauh lebih baik dibandingkan papua, maluku, dan Nusa Tenggara Timur yang indeks literasinya di bawah 50 poin. Keterbatasan akses internet dan fasilitas literasi digital di daerah 3T menyebabkan masyarakat lebih rentan terhadap penyebaran hoaks dan kejahatan siber.

Penelitian [22] menegaskan bahwa hanya 30% sekolah di daerah terpencil memiliki fasilitas TIK memadai, namun pelatihan berbasis praktik dapat meningkatkan kemampuan guru hingga 60%. Hal ini menegaskan pentingnya pendekatan low-tech dan berbasis komunitas untuk menjangkau masyarakat di wilayah dengan keterbatasan akses.

4.2.2. Rendahnya Kesadaran Keamanan Siber

Berdasarkan data [23], selama Januari – Mei 2024 terdapat 74 juta anomali trafik, di

mana 59,7% di antaranya merupakan aktivitas malware. Selain itu, [24] mencatat peningkatan 220% kasus *phising* domain .id dalam satu kuartal, dan [25] melaporkan kebocoran 6 juta data NPWP, termasuk milik Presiden Jokowi.

Kasus – kasus ini memperlihatkan lemahnya implementasi UU Perlindungan Data Pribadi (UU PDP 2022) dan belum terbentuknya lembaga pengawas independen. Rendahnya kesadaran digital juga tercermin dalam data [26], yang mencatat kerugian masyarakat sebesar Rp. 4,6 triliun akibat penipuan daring dalam 10 bulan.

4.2.3. Upaya Edukasi dan Kebijakan Pemerintah

Pemerintah telah berupaya melalui GNLD Siberkreasi dan kebijakan strategis BSSN 2017 yang menekankan lima fokus utama: ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan, dan ekonomi digital aman.

Namun, penelitian [27] menunjukkan bahwa regulasi siber nasional masih belum terintegrasi antara UU ITE, UU PDP, dan kebijakan BSSN. Kelemahan koordinasi antar lembaga (Kominfo, BSSN, Polri, dan OJK) menjadi hambatan utama dalam penerapan kebijakan perlindungan data secara efektif.

4.2.4. Analisis Tematik Gabungan

Hasil telaah seluruh dokumen dan artikel menghasilkan tujuh tema besar yang saling berhubungan. Tabel 1 merangkum hasil analisis tematik gabungan.

Tabel 1. Hasil Analisis Tematik

Tema Utama	Sumber & Bukti Empiris	Temuan Kunci	Implikasi Akademik/Kebijakan
Literasi Digital & Ketahanan Siber	Kominfo, BPS, Wijaksono (2023), Surbakti (2024)	Literasi digital meningkat tapi belum merata; pelatihan lokal efektif	Perluasan edukasi berbasis komunitas dan media low-tech
Kebijakan Perlindungan Data	Kompas, Novita dkk (2024), BSSN	Implementasi UU PDP belum optimal	Perlu percepatan pembentukan lembaga pelindungan data
Ancaman Siber	CNN, Tempo, Liputan6	Lonjakan malware, phishing, dan scam digital	Diperlukan sistem deteksi dan respon siber nasional
Kesenjangan Digital	APJII, BPS, Wijaksono (2023)	Perbedaan infrastruktur antar wilayah tinggi	Strategi edukasi hybrid dan pemerataan infrastruktur
Penegakan Hukum	Liputan6, BSSN	Kasus menurun tapi modus meningkat	Penguatan koordinasi Kominfo–Polri
Budaya Aman Digital	Kominfo, Surbakti (2024)	Kesadaran etika dan tanggung jawab digital masih rendah	Perlu kampanye budaya aman digital nasional
Ekonomi Digital & Kepercayaan Publik	Liputan6, Kompas	Keamanan data memengaruhi kepercayaan transaksi	Keamanan siber sebagai fondasi ekonomi digital

4.3. Analisis Hubungan Antartema

Mengacu pada tahapan analisis [19], tahap interpretation menghasilkan pola hubungan antartema sebagai berikut:

(1) Pola Kausal
Rendahnya literasi digital menyebabkan meningkatnya kerentanan terhadap phising, scam, dan kebocoran data [21], [26], [25].

(2) Pola Interdependensi
Regulasi siber dan budaya aman digital saling memengaruhi kebijakan tanpa kesadaran sosial tidak efektif, dan kesadaran sosial tanpa dukungan hukum tidak berdaya.

(3) Pola Sinergi
Literasi, regulasi, dan kolaborasi lintas sektor membentuk tiga pilar utama keamanan siber nasional:

- Pilar sosial: peningkatan literasi digital masyarakat
- Pilar regulatif: harmonisasi UU dan kelembagaan
- Pilar teknis: penguatan deteksi dan infrastruktur siber

Hubungan ini menunjukkan bahwa keberhasilan keamanan siber bergantung pada keterpaduan edukasi, kebijakan, dan teknologi.

4.4. Pengembangan Solusi Edukasi

Berdasarkan hasil analisis, solusi yang dikembangkan berfokus pada edukasi keamanan siber berbasis komunitas dan media low-tech. Pendekatan ini dirancang untuk menjangkau masyarakat di daerah dengan keterbatasan infrastruktur internet.

Media yang digunakan mencakup pamflet, poster, modul pelatihan langsung, serta simulasi sederhana mengenai keamanan data pribadi dan deteksi penipuan digital.

Model ini dikembangkan dengan prinsip community-based learning, di mana masyarakat menjadi pelaku aktif dalam meningkatkan kesadaran keamanan siber melalui kegiatan lokal, bukan hanya sebagai penerima informasi.

4.5. Validasi dan Rekomendasi

Hasil studi dokumen dan analisis tematik memberikan dasar kuat untuk validasi kebijakan dan edukasi keamanan siber di Indonesia. Tiga rekomendasi strategis dihasilkan:

(1) Peningkatan literasi digital masyarakat secara inklusif, terutama di wilayah dengan indeks literasi rendah melalui pendekatan komunitas.
(2) Percepatan pembentukan lembaga pelindungan data pribadi independen untuk menjamin penegakan UU PDP.
(3) Integrasi kolaboratif lintas sektor antara pemerintah, akademisi, dan masyarakat sipil untuk membangun budaya aman digital nasional.

Pembahasan

Hasil penelitian ini memperkuat temuan sebelumnya [27], bahwa keamanan siber di Indonesia tidak hanya ditentukan oleh kecanggihan teknologi, tetapi juga oleh kapasitas literasi dan kesadaran sosial masyarakat digital.

Pendekatan berbasis komunitas dan *low-tech* terbukti lebih relevan dengan konteks Indonesia yang memiliki kesenjangan akses dan tingkat literasi yang beragam.

Dengan demikian, keberhasilan strategi keamanan siber nasional bergantung pada kolaborasi tiga unsur utama, yaitu edukasi masyarakat, regulasi yang adaptif, dan koordinasi antar lembaga.

5. KESIMPULAN

Berdasarkan dokumen dan hasil analisis yang telah diperoleh, didapatkan beberapa kesimpulan yaitu:

a. Meskipun penetrasi internet Indonesia telah mencapai lebih dari 78% (APJII), kesenjangan antara wilayah urban dan rural serta daerah 3T masih tinggi. Kondisi ini berdampak langsung pada rendahnya literasi digital dan tingginya kerentanan terhadap kejahatan siber di wilayah tertinggal.
b. Lonjakan kasus phising, malware, dan online scam yang menyebabkan kerugian hingga triliunan rupiah menunjukkan bahwa sebagian besar masyarakat belum menerapkan praktik keamanan dasar seperti autentikasi ganda dan verifikasi sumber informasi.
c. Program GNLD Siberkreasi, Strategi Keamanan Siber Nasional, serta UU Perlindungan Data Pribadi (UU PDP) telah membentuk kerangka regulatif yang kuat. Namun, belum terbentuknya lembaga pengawas data pribadi dan belum sinkronnya kebijakan antar lembaga (Kominfo, BSSN, Polri, OJK) menghambat efektivitas pelaksanaan kebijakan.
d. Hasil berbagai penelitian menunjukkan bahwa pelatihan berbasis lokal dan metode *low-tech* berhasil meningkatkan literasi digital hingga 60% di daerah minim infrastruktur. Pendekatan ini lebih kontekstual dan sesuai dengan kondisi sosial-budaya masyarakat Indonesia.
e. Upaya membangun ekosistem digital yang aman harus mencakup tiga pilar utama: peningkatan literasi digital masyarakat, harmonisasi regulasi siber lintas lembaga, dan kerja sama multi-sektor (pemerintah, akademisi, industri, dan masyarakat). Integrasi ini menjadi kunci menuju

ketahanan digital nasional yang inklusif, adaptif, dan berkelanjutan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak terkait yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] A. M. A. Saputra, L. P. I. Kharisma, A. A. Rizal, M. I. Burhan, and N. W. Purnawati, *Teknologi Informasi : Peranan TI dalam berbagai bidang*. PT. Sonpedia Publishing Indonesia, 2023.

[2] S. F. Zis, N. Effendi, and E. R. Roem, "Perubahan Perilaku Komunikasi Generasi Milenial dan Generasi Z di Era Digital," *Satwika: Kajian Ilmu Budaya dan Perubahan Sosial*, vol. 5, no. 1, pp. 69–87, Apr. 2021.

[3] A. Martin, *Lembaga Ketahanan Nasional Republik Indonesia*. 2024.

[4] A. Putri, N. Sari, P. Fajrina, and S. Aisyah, "Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering)," *Jurnal Pengabdian Nasional (JPN) Indonesia*, vol. 6, no. 1, pp. 38–52, Nov. 2024.

[5] R. Fauji Setiawan, "Analisis Sentimen Isu Ancaman Siber Menggunakan Algoritma Multi-layer Perceptron," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 3, pp. 1296–1302, Jul. 2025.

[6] P. Serianti, D. Ria, Y. Tb, and R. Albar, "Peningkatan Literasi Digital Siswa SMA melalui Pelatihan Pemanfaatan Teknologi Informasi di Era Revolusi Industri 4.0 Enhancing Digital Literacy of High School Students through Information Technology Training in the 4.0 Industrial Revolution Era," *Jurnal Pengabdian Masyarakat (INOTEC)*, vol. 6, no. 1, 2024.

[7] H. S. Wibowo, *Pengembangan Teknologi Media Pembelajaran: Merancang Pengalaman Pembelajaran yang Inovatif dan Efektif*. Tiram Media, 2023.

[8] Firman, F. Inovasi dalam manajemen pendidikan Islam untuk meningkatkan kualitas pembelajaran di era pendidikan digital. Jurnal Review Pendidikan dan Pengajaran (JRPP), 7(3), 9035-9044. (2024).

[9] J. L. Putra, M. Raharjo, and E. Fitri, "Analisis Ancaman Siber dan Persiapan Pemuda Karang Taruna Kelurahan Rengas dalam Menghadapi Risiko Keamanan Siber," *Indonesian Journal for Social Responsibility*, vol. 6, no. 2, pp. 151–163, 2024.

[10] A. R. Kelrey and A. Muzaki, "Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan," vol. 2, no. 2, pp. 2615–8442, 2019.

[11] H. S. Wibowo, *Penguatan Literasi Digital: Menguasai Dunia Literasi di Era Digitalisasi*. Tiram Media, 2023.

[12] C. M. Zuhra, M. Daud, S. Sabrina, C. Faizah, N. Fitria, and Y. Yanti, *Literasi Digital Berbasis Kearifan Lokal Sabang dalam Pembelajaran Bahasa Inggris*. Mega Press Nusantara, 2024.

[13] lyas Marwal, *Wakaf Digital: Meretas Peluang Baru Dalam Era Teknologi*. Penerbit Tahta Media, 2024.

[14] F. T. S. Utomo, "Inovasi Media Pembelajaran Interaktif Untuk Meningkatkan Efektivitas Pembelajaran Era Digital Di Sekolah Dasar," *Pendas: Jurnal Ilmiah Pendidikan Dasar*, vol. 8, no. 2, pp. 3635–3645, 2023.

[15] M. Azizi, S. Ahmad, R. Ernayani, S. P. Anantadjaya, and W. Lestari, "Peningkatan Literasi Keuangan Untuk Generasi Muda," *Communnity Development Journal*, vol. 5, no. 5, 2024.

[16] D. Julianti, "Strategi Kebijakan Penguatan Pelayanan Publik Dan Pengawasan Perizinan Berusaha Dengan Aplikasi Berbasis Teknologi Informasi," *Kybernology Jurnal Ilmu Pemerintahan dan Administrasi Publik*, vol. 2, no. 2, pp. 324–363, 2024.

[17] H. A. Setiawan, "Pengaruh Literasi Digital terhadap Pemanfaatan E-Commerce pada Hasil Pertanian Influence of Digital Literacy on the Utilization of E-Commerce in Agricultural Products," *Ju Jurnal Kolaboratif Sains*, vol. 7, no. 5, pp. 1598–1607, 2024.

[18] D. A. R. Widyastuti, R. Nuswantoro, and T. A. P. Sidhi, "Literasi Digital Pada Perempuan Pelaku Usaha Produktif Di Daerah Istimewa Yogyakarta".

[19] R. Nurislaminingsih and H. Heriyanto, *Riset Kualitatif untuk Pemula Teknik Analisis Data*. CV. Intishar Publishing, 2024.

[20] Kominfo, "Laporan Kinerja Kominfo," 2023.

[21] APJII, "Survei Internet Indonesia Tahap 1," Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), 2023, pp. 1–10.

[22] A. Wijaksono, "Peningkatan Literasi Digital Melalui Pelatihan Guru Di Daerah Terpencil," *Jurnal Akselerasi Merdeka Belajar dalam Pengabdian Orientasi Masyarakat*, vol. 1, no. 2, pp. 62–68, 2023.

[23] H. Siburian, "Strategi Keamanan Siber Nasional," Badan Siber dan Sandi Negara (BSSN).

[24] M. F. Lahur, "IDADX Terima 69.117 Laporan Kejahatan Phishing Domain .id hingga 31 Maret," Tempo.co.
[25] A. P. Saptohutomo, "Kebocoran Data Berulang, Seberapa Siap Indonesia Menerapkan UU PDP? ," Kompas.com.
[26] A. Anugrahadi, "Polri Tindak 3.331 Kasus Kejahatan di Ruang Siber Sepanjang Tahun 2024," Liputan6.
[27] D. Novita, M. Mulyono, and A. Retnowati, "Perkembangan Hukum Siber di Indonesia: Studi Literatur tentang Tantangan dan Solusi Keamanan Nasional," *INNOVATIVE: Journal Of Social Science Research*, vol. 4, no. 6, pp. 1–8, 2024.
[28] CNN Indonesia, "BSSN Deteksi 44 Juta Aktivitas Malware Hingga Mei 2024," CNN Indonesia.
[29] H. Purnomo, "Kerugian Warga RI Kena Penipuan Online Capai Rp 4,6 T dalam 10 Bulan," detik.com.
[30] F. P. S. Surbakti, "Edukasi Keamanan Siber Berdigital dengan Aman," *Prima Abdika: Jurnal Pengabdian Masyarakat*, vol. 4, no. 4, pp. 868–878, Dec. 2024.
[31] I. F. Ahmad, "Urgensi Literasi Digital di Indonesia pada Masa Pandemi COVID-19: Sebuah Tinjauan Sistematis," *Nusantara: Jurnal Pendidikan Indonesia*, vol. 2, no. 1, pp. 1–18, Jan. 2022.
[32] BPS, "Indeks Pembangunan Literasi Masyarakat dan Unsur Penyusunnya Menurut Provinsi," 2024.
[33] Kominfo, "Indonesia Terkoneksi Semakin Digital, Semakin Maju," 2020.