Jurnal Sains Dan Teknologi Informasi
Vol 5, No 3, Juni 2026, Hal 155-163
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v5i3.10311
Website https://ejurnal.seminar-id.com/index.php/jussi

Analisis Keamanan Digital Perguruan Tinggi Terhadap Ancaman Siber Generasi Z melalui Metode *Defense-In-Depth*

Joko Triyanto, Farros Yumna Prabowo, Muhammad Hafizh Nur Hidayat, Ramzy Alfatoni, Ahmad Baehaqi*

Fakultas Sains dan Teknologi, Program Studi Teknologi Informasi, Universitas Islam Negeri Salatiga, Jawa Tengah, Indonesia
Email: [1]joko.triyanto@uinsalatiga.ac.id, [2]prabowofarros@email.com, [3]nurhidayathafizh375@gmail.com,
[4]ramzyalfa099@gmail.com, [5,*]ahmadbaehaqi987@gmail.com
(* : coressponding author)

Abstrak−Transformasi digital pada perguruan tinggi telah meningkatkan penggunaan teknologi informasi dalam aktivitas akademik, komunikasi, dan pengelolaan data digital. Kondisi tersebut memberikan berbagai kemudahan dalam sistem pendidikan, namun di sisi lain juga meningkatkan ancaman keamanan siber terhadap Generasi Z sebagai pengguna utama teknologi digital di lingkungan kampus. Penelitian ini bertujuan menganalisis pertahanan siber perguruan tinggi dalam menghadapi ancaman siber pada Generasi Z serta mengidentifikasi bentuk ancaman digital yang paling dominan menyerang mahasiswa. Pendekatan yang digunakan bersifat kualitatif melalui studi kepustakaan (*library research*) dengan menelaah beragam jurnal ilmiah, artikel akademik, dan literatur seputar keamanan siber, literasi digital, serta perilaku digital Generasi Z terbitan tiga tahun terakhir (2023–2026). Data yang terhimpun dianalisis secara deskriptif kualitatif melalui tahap reduksi, klasifikasi, interpretasi, dan sintesis untuk merumuskan model pertahanan siber kampus berlapis (*Defense-in-Depth*). Hasil penelitian menunjukkan bahwa tingginya intensitas penggunaan media sosial, rendahnya literasi keamanan digital, serta perilaku *oversharing* menjadi faktor utama meningkatnya kerentanan siber pada Generasi Z. Selain itu, *phishing*, pencurian data pribadi, *social engineering*, dan *cyber radicalism* menjadi bentuk ancaman siber yang paling dominan pada lingkungan perguruan tinggi. Hasil analisis juga menunjukkan bahwa hanya 40% mahasiswa mampu mengenali ancaman *phishing* secara mandiri, sedangkan edukasi keamanan siber terbukti meningkatkan pemahaman keamanan digital dengan kenaikan pengetahuan keamanan data 8,33 poin dan pemahaman risiko teknologi 10,17 poin. Oleh karena itu, penguatan literasi keamanan siber, edukasi digital, dan pengembangan sistem pertahanan siber kampus yang adaptif menjadi langkah strategis dalam meningkatkan keamanan digital perguruan tinggi.

Kata Kunci: Keamanan Siber, Generasi Z, Pertahanan Siber, Perguruan Tinggi, Literasi Digital

Abstract−*Digital transformation in higher education has increased the use of information technology in academic activities, communication, and digital data management. This condition provides various conveniences in the education system; however, it also increases cybersecurity threats toward Generation Z as the primary users of digital technology within universities. This study aims to analyze the cyber defense of higher education institutions in dealing with cyber threats among Generation Z and to identify the most dominant forms of digital threats targeting students. A qualitative approach was adopted through a library research method, examining a range of scholarly journals, academic articles, and literature on cybersecurity, digital literacy, and the digital behavior of Generation Z published within the last three years (2023–2026). The collected data were analyzed descriptively and qualitatively through reduction, classification, interpretation, and synthesis to formulate a layered campus cyber defense model (Defense-in-Depth). The findings indicate that the high intensity of social media usage, low cybersecurity literacy, and oversharing behavior are the main factors contributing to increasing cyber vulnerability among Generation Z. In addition, phishing, personal data theft, social engineering, and cyber radicalism are identified as the most dominant cyber threats within higher education environments. The analysis also reveals that only 40% of students are able to independently recognize phishing threats, while cybersecurity education improves data security knowledge by 8.33 points and technological risk understanding by 10.17 points. Therefore, strengthening cybersecurity literacy, digital education, and the development of adaptive campus cyber defense systems are strategic steps in enhancing digital security in higher education institutions.*

Keywords: *Cybersecurity, Generation Z, Cyber Defense, Higher Education, Digital Literacy*

1. PENDAHULUAN

Permasalahan keamanan siber di lingkungan perguruan tinggi menjadi semakin serius karena institusi pendidikan tinggi menyimpan berbagai data strategis, mulai dari data akademik mahasiswa, identitas civitas akademika, hasil penelitian, hingga data keuangan institusi. Serangan siber terhadap sistem pendidikan tidak hanya menimbulkan kerugian teknis, tetapi juga dapat mengganggu stabilitas layanan akademik dan menurunkan tingkat kepercayaan publik terhadap keamanan kampus. Kondisi ini diperberat oleh karakteristik Generasi Z sebagai pengguna utama teknologi digital yang memiliki intensitas penggunaan teknologi sangat tinggi tetapi tingkat kesadaran keamanan digitalnya belum optimal [1]. Rendahnya pemahaman terhadap praktik keamanan digital, seperti penggunaan kata sandi yang lemah, ketidaktahuan terhadap ancaman *phishing*, serta belum dimanfaatkannya fitur *two-factor authentication*, menjadi salah satu penyebab utama meningkatnya kejahatan siber [2]. Dengan demikian, perguruan tinggi dituntut membangun sistem pertahanan siber yang tidak hanya bertumpu pada kekuatan teknologi, tetapi juga pada penguatan literasi keamanan digital mahasiswa.

Urgensi kajian ini kian terasa apabila ditinjau dari kecenderungan ancaman siber di tingkat nasional. Data Badan Siber dan Sandi Negara (BSSN) memperlihatkan kenaikan anomali trafik siber yang amat curam pada beberapa tahun terakhir, dan sektor pendidikan kerap menjadi salah satu sasaran yang paling sering dibidik [3]. Peningkatan ini menegaskan bahwa ruang digital telah menjadi medan baru yang rentan dieksploitasi, sehingga tata kelola keamanan siber nasional menjadi kebutuhan mendesak [4]. Ancaman tersebut pun tidak lagi terbatas pada pencurian data atau peretasan

Jurnal Sains Dan Teknologi Informasi
Vol 5, No 3, Juni 2026, Hal 155-163
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v5i3.10311
Website https://ejurnal.seminar-id.com/index.php/jussi

sistem, melainkan meluas ke penyebaran propaganda digital, manipulasi informasi, dan radikalisasi daring yang memanfaatkan besarnya populasi pengguna internet di Indonesia [5].

Di sisi lain, ancaman siber modern menuntut sistem pertahanan yang lebih adaptif dan terintegrasi. Penanganan ancaman digital tidak dapat dilakukan secara sektoral karena melibatkan aspek teknologi, sumber daya manusia, regulasi, dan kolaborasi lintas institusi secara bersamaan [6]. Lemahnya koordinasi, terbatasnya kapasitas teknologi, dan minimnya literasi keamanan digital kerap menjadi titik lemah strategi penanganan keamanan siber di Indonesia [7]. Oleh karena itu, perguruan tinggi memerlukan model pertahanan siber yang holistik, yaitu yang memadukan penguatan sistem teknologi, kebijakan institusi, serta peningkatan kesadaran keamanan digital mahasiswa sebagai satu kesatuan.

Untuk memperjelas kerangka analisis, beberapa konsep utama dalam penelitian ini perlu didefinisikan terlebih dahulu. *Cyber defense* (pertahanan siber) dimaknai sebagai keseluruhan upaya, strategi, dan mekanisme yang dilakukan suatu entitas untuk melindungi sistem, jaringan, dan data dari serangan siber, baik melalui pendekatan teknologi maupun penguatan sumber daya manusia [8]. Dalam konteks penelitian ini, *cyber defense* perguruan tinggi tidak dipahami sebatas perangkat keamanan teknis, melainkan mencakup pula kebijakan, budaya keamanan, dan literasi digital seluruh penggunanya.

Ancaman siber (*cyber threat*) merupakan segala bentuk tindakan yang memanfaatkan kelemahan sistem teknologi maupun faktor manusia untuk memperoleh akses, merusak, mencuri, atau menyalahgunakan data dan informasi, yang cakupannya terus berkembang seiring kemajuan teknologi. Salah satu wujud nyata dari ancaman tersebut adalah *cyber espionage*, yaitu kejahatan siber yang memanfaatkan jaringan internet dan aplikasi media sosial untuk memata-matai, menyadap, serta mengambil data elektronik milik pihak lain secara diam-diam [9]. Perguruan tinggi dalam penelitian ini dipandang sebagai institusi pendidikan dengan arus informasi yang tinggi serta pengelola aset kritis berupa data akademik dan data pribadi sivitas akademika, sehingga menjadi salah satu lingkungan yang paling rentan terhadap serangan siber [10]. Adapun Generasi Z didefinisikan sebagai generasi yang lahir dan tumbuh bersama perkembangan teknologi digital (*digital natives*) sehingga memiliki kemampuan adaptasi teknologi yang tinggi. Kemampuan tersebut tidak selalu berbanding lurus dengan *literasi digital*, yaitu kecakapan memahami, menilai, dan menggunakan informasi digital secara aman, kritis, dan bertanggung jawab [11]. Kesenjangan antara kemampuan teknis dan literasi keamanan inilah yang menjadi titik tolak analisis dalam penelitian ini.

Sejumlah penelitian terdahulu telah mengkaji isu keamanan siber dari berbagai sudut pandang. Pendekatan berbasis komunitas terbukti mampu mentransformasi generasi muda dari pengguna digital pasif menjadi pelindung keamanan siber yang aktif [12], sementara penguatan kapasitas sumber daya manusia dan kepemimpinan digital dinilai sebagai faktor penting dalam membangun ekosistem keamanan siber yang berkelanjutan [13]. Pada tataran perilaku, tingginya aktivitas transaksi dan konsumsi digital Generasi Z belum diimbangi literasi keamanan yang memadai [14], sedangkan dorongan memperoleh validasi sosial mendorong perilaku berbagi data pribadi yang meningkatkan risiko pencurian identitas [15]. Beberapa studi menunjukkan bahwa edukasi keamanan siber yang terstruktur efektif meningkatkan pengetahuan dan kewaspadaan pelajar terhadap ancaman digital [16], serta bahwa rendahnya literasi digital membuat generasi muda rentan terhadap disinformasi dan ancaman non-militer [17].

Penelitian lain memetakan kesadaran mahasiswa terhadap keamanan siber dan menemukan bahwa sebagian besar belum mampu mengenali serangan secara mandiri [18]. Pola serupa ditemukan pada kasus *phishing* yang memanfaatkan tingginya penggunaan media sosial di kalangan mahasiswa [19], bahkan ancaman telah berkembang ke ranah ideologis berupa *cyber radicalism* yang menyebarkan propaganda melalui media sosial untuk menyasar Generasi Z [20]. Meskipun demikian, sebagian besar penelitian tersebut masih membahas keamanan siber dalam konteks nasional, regulasi hukum, atau edukasi masyarakat secara umum, dan belum secara khusus mengintegrasikan perilaku digital Generasi Z ke dalam sistem pertahanan siber institusi pendidikan tinggi.

Berdasarkan tinjauan tersebut, terdapat kesenjangan penelitian (*research gap*), yaitu masih terbatasnya kajian yang menganalisis pertahanan siber perguruan tinggi dengan menempatkan karakteristik Generasi Z sebagai variabel utama. Kebaruan (*novelty*) penelitian ini terletak pada upaya menjembatani aspek teknis pertahanan siber dengan aspek perilaku dan literasi digital mahasiswa dalam satu kerangka analisis yang utuh. Atas dasar itu, penelitian ini bertujuan untuk: (1) menganalisis sistem pertahanan siber perguruan tinggi dalam menghadapi ancaman siber pada Generasi Z; (2) mengidentifikasi bentuk ancaman digital yang paling dominan menyerang mahasiswa; serta (3) merumuskan arah penguatan keamanan siber berbasis literasi digital dan kesadaran pengguna agar tercipta pertahanan siber kampus yang lebih adaptif, preventif, dan berkelanjutan.

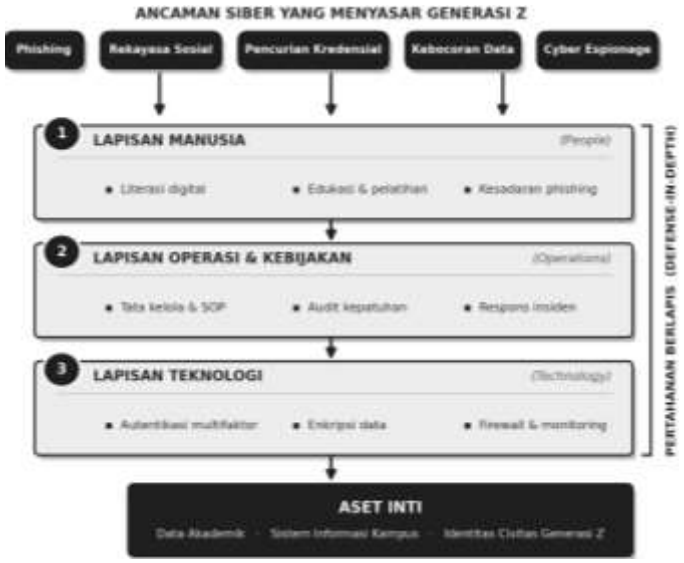
2. METODOLOGI PENELITIAN

2.1 Pendekatan Penelitian

Kajian ini dirancang dengan paradigma kualitatif yang ditopang oleh studi kepustakaan (*library research*) untuk menelaah pertahanan siber perguruan tinggi terhadap ancaman yang dihadapi Generasi Z. Paradigma kualitatif dipilih karena titik berat kajian terletak pada penelaahan mendalam atas konsep, teori, serta hasil riset terdahulu seputar keamanan siber di ranah pendidikan tinggi, bukan pada pengukuran angka. Studi kepustakaan ditempuh sebab penelitian tidak menghimpun data lapangan, melainkan menjadikan beragam rujukan akademik sebagai sumber utama, sebagaimana lazim diterapkan pada kajian keamanan siber berbasis literatur terkini [16].

Jurnal Sains Dan Teknologi Informasi
Vol 5, No 3, Juni 2026, Hal 155-163
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v5i3.10311
Website https://ejurnal.seminar-id.com/index.php/jussi

Metode yang digunakan untuk menyelesaikan masalah dalam penelitian ini adalah strategi pertahanan berlapis (*Defense-in-Depth*), yaitu pendekatan keamanan siber yang menyusun beberapa kontrol pengamanan independen secara bertingkat sehingga kelemahan pada satu lapisan dapat ditutup oleh lapisan lainnya [21]. Kajian pustaka terhadap metode ini menunjukkan bahwa *Defense-in-Depth* membagi pertahanan ke dalam tiga lapisan utama, yakni lapisan manusia (*people*), lapisan teknologi (*technology*), serta lapisan operasi dan kebijakan (*operations*) [22]. Lapisan manusia menekankan penguatan literasi dan edukasi keamanan siber bagi Generasi Z, lapisan teknologi mencakup autentikasi multifaktor, enkripsi, dan pemantauan jaringan, sedangkan lapisan operasi dan kebijakan mencakup tata kelola, regulasi, serta prosedur respons insiden [21]. Ketiga lapisan tersebut diterapkan untuk memetakan setiap pola ancaman siber yang dihadapi Generasi Z di perguruan tinggi ke dalam strategi pertahanan yang saling melengkapi. Kerangka metode *Defense-in-Depth* yang digunakan dalam penelitian ini digambarkan pada Gambar 1.



Gambar 1. Model pertahanan berlapis (*Defense-in-Depth*) keamanan siber perguruan tinggi

Gambar 1 menunjukkan bahwa metode *Defense-in-Depth* menempatkan literasi Generasi Z sebagai lapisan terluar, diikuti lapisan operasi dan kebijakan, kemudian lapisan teknologi yang langsung melindungi aset inti berupa data dan sistem informasi kampus. Susunan berlapis ini memastikan bahwa apabila satu lapisan gagal, lapisan berikutnya tetap menahan serangan sehingga risiko terhadap aset inti dapat ditekan.

2.2 Sumber Data Penelitian

Data dalam kajian ini bersumber dari aneka literatur ilmiah yang relevan dengan topik, meliputi jurnal nasional dan internasional, artikel ilmiah, buku, prosiding seminar, serta dokumen penelitian yang membahas keamanan siber (*cyber security*), ancaman siber pada perguruan tinggi, perilaku digital Generasi Z, dan strategi pertahanan siber dalam dunia pendidikan. Literatur diperoleh melalui basis data akademik seperti Google Scholar, Scopus, dan SINTA. Penelitian ini mengutamakan sumber pustaka yang diterbitkan dalam tiga tahun terakhir (2023–2026) agar data bersifat relevan dengan perkembangan ancaman siber terkini. Pemilihan sumber dilakukan berdasarkan relevansi isi, kejelasan metode, validitas data, dan kesesuaian hasil penelitian dengan fokus kajian.

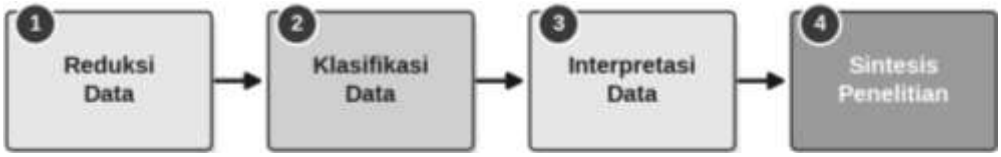
2.3 Teknik Pengumpulan Data

Penghimpunan data ditempuh dengan teknik dokumentasi yang dipadukan dengan penelusuran literatur (*literature searching*), sebagaimana ditempuh penelitian terdahulu yang menganalisis strategi keamanan siber melalui kajian pustaka [7]. Pencarian artikel ilmiah menggunakan kata kunci seperti “cyber security”, “cyber defense”, “higher education cyber security”, “Generasi Z”, “digital literacy”, dan “cyber threats”. Literatur yang ditemukan diseleksi berdasarkan kesesuaian judul, abstrak, isi, tujuan, metode, dan hasil penelitian dengan fokus kajian. Artikel yang tidak relevan, duplikatif, atau tidak memiliki akses penuh (*full text*) dieliminasi pada proses seleksi. Selanjutnya dilakukan pencatatan data penting dari setiap sumber, seperti nama penulis, tahun, metode, dan hasil penelitian, untuk mempermudah analisis.

2.4 Teknik Analisis Data

Analisis data ditempuh secara deskriptif kualitatif melalui empat tahapan yang saling berurutan, yakni reduksi, klasifikasi, interpretasi, dan sintesis [4]. Pada tahap reduksi, data disaring sehingga hanya yang relevan dengan fokus kajian yang dipertahankan; pada tahap klasifikasi, data dikelompokkan menurut tema seperti ancaman siber, kerentanan sistem digital kampus, literasi keamanan, serta strategi pertahanan; pada tahap interpretasi, keterkaitan antardata dimaknai untuk memperoleh pemahaman yang lebih utuh; dan pada tahap sintesis, seluruh temuan dirangkai menjadi pembahasan yang runtut serta menyeluruh. Rangkaian tahapan analisis tersebut digambarkan pada Gambar 2.

Jurnal Sains Dan Teknologi Informasi
Vol 5, No 3, Juni 2026, Hal 155-163
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v5i3.10311
Website https://ejurnal.seminar-id.com/index.php/jussi



Gambar 2. Alur tahapan analisis data

Gambar 2 memperlihatkan bahwa proses analisis bergerak dari reduksi data menuju sintesis penelitian; setiap tahap menyaring dan memadatkan temuan sehingga pada akhirnya menghasilkan pembahasan yang utuh dan terstruktur.

2.5 Prosedur Penelitian

Prosedur penelitian disusun secara sistematis dalam lima tahap yang merujuk pada alur kajian pustaka yang banyak digunakan dalam penelitian keamanan siber [16]. Tahap pertama adalah identifikasi masalah terkait meningkatnya ancaman siber pada perguruan tinggi dan tingginya aktivitas digital Generasi Z. Tahap kedua adalah pengumpulan sumber pustaka yang relevan melalui basis data akademik. Tahap ketiga adalah seleksi dan klasifikasi literatur berdasarkan relevansi dengan fokus kajian. Tahap keempat adalah analisis data melalui proses reduksi hingga sintesis. Tahap terakhir adalah sintesis temuan ke dalam model pertahanan berlapis (Defense-in-Depth) sebagai solusi yang diusulkan, disertai penarikan kesimpulan dan perumusan rekomendasi strategis. Keseluruhan tahapan prosedur penelitian digambarkan pada Gambar 3.

Gambar 3. Tahapan prosedur penelitian

Sebagaimana ditunjukkan pada Gambar 3, keseluruhan prosedur penelitian dirangkum dalam lima tahap berurutan, mulai dari identifikasi masalah hingga sintesis model pertahanan berlapis (Defense-in-Depth) sebagai solusi yang diusulkan, sehingga proses penelitian dapat ditelusuri secara sistematis. Penerapan solusi atau metode terlihat jelas pada tahap kelima bagan tersebut, yaitu ketika seluruh temuan literatur disintesiskan ke dalam metode *Defense-in-Depth*; pada tahap inilah pola ancaman siber Generasi Z yang teridentifikasi dipetakan ke dalam tiga lapisan pertahanan, yakni lapisan manusia, lapisan teknologi, serta lapisan operasi dan kebijakan, sehingga bagan tahapan penelitian sekaligus memperlihatkan bagaimana metode yang digunakan diaplikasikan untuk menyelesaikan masalah penelitian.

3. HASIL DAN PEMBAHASAN

Pembahasan pada bagian ini merupakan hasil penerapan empat tahap analisis data yang telah diuraikan pada metodologi, yakni reduksi, klasifikasi, interpretasi, dan sintesis, terhadap seluruh literatur yang terhimpun. Data terlebih dahulu direduksi untuk memilih temuan yang relevan, kemudian diklasifikasikan menurut tema kerentanan dan pola ancaman, ditafsirkan keterkaitannya, dan akhirnya disintesiskan menjadi dua fokus pembahasan, yaitu meningkatnya kerentanan siber Generasi Z serta pola ancaman siber dan strategi pertahanannya.

3.1 Transformasi Digital Perguruan Tinggi dan Meningkatnya Kerentanan Siber Generasi Z

Transformasi digital telah mengubah pola aktivitas perguruan tinggi menjadi ekosistem yang sepenuhnya terintegrasi dengan teknologi informasi. Sistem pembelajaran berbasis *Learning Management System* (LMS), media sosial akademik, layanan administrasi daring, penyimpanan berbasis *cloud computing*, hingga pemanfaatan kecerdasan buatan (*Artificial Intelligence*) telah menjadi tulang punggung penyelenggaraan pendidikan tinggi modern. Kemudahan ini memberikan manfaat besar bagi efektivitas pembelajaran, percepatan komunikasi akademik, dan keterbukaan akses informasi. Namun, setiap penambahan kanal digital sekaligus memperluas permukaan serangan (*attack surface*) yang dapat dieksploitasi. Generasi Z, sebagai kelompok pengguna paling dominan di lingkungan kampus, justru menjadi titik paling terpapar dalam ekosistem ini karena seluruh aktivitas akademiknya berlangsung di ruang digital.

Perluasan ruang digital ini sekaligus memperbanyak aset bernilai yang harus dilindungi. Data identitas mahasiswa dan dosen, basis data akademik, sistem keuangan, arsip hasil penelitian, hingga kredensial akun layanan kampus seluruhnya tersimpan dan dipertukarkan secara daring. Setiap aset tersebut memiliki nilai ekonomi maupun strategis sehingga menarik bagi pelaku kejahatan siber. Hasil analisis menunjukkan bahwa semakin banyak titik akses dan jenis data yang dikelola secara digital, semakin kompleks pula upaya perlindungan yang dibutuhkan, dan semakin besar konsekuensi yang muncul apabila salah satu titik tersebut berhasil ditembus.

Jurnal Sains Dan Teknologi Informasi
Vol 5, No 3, Juni 2026, Hal 155-163
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v5i3.10311
Website https://ejurnal.seminar-id.com/index.php/jussi

Posisi Generasi Z sebagai kelompok paling terpapar dapat dibaca dari pola penggunaan internet nasional. Berdasarkan rilis Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada 2025, tingkat penetrasi internet di Tanah Air menyentuh 80,66% dari keseluruhan populasi, dengan Generasi Z sebagai penyumbang pengguna terbanyak serta rata-rata durasi berinternet maupun bermedia sosial mencapai 5,7 jam setiap hari. Angka ini menempatkan Generasi Z pada intensitas paparan digital tertinggi dibanding kelompok usia lain. Dari analisis penelitian ini, intensitas yang tinggi tersebut bukan sekadar indikator literasi teknologi, melainkan juga pengganda risiko: semakin lama dan semakin luas keterlibatan digital seseorang, maka semakin besar pula peluangnya berhadapan dengan upaya manipulasi, pencurian data, maupun serangan berbasis rekayasa sosial.

Persoalan utamanya terletak pada kesenjangan antara kemampuan teknis dan kesadaran keamanan. Generasi Z menguasai perangkat digital secara intuitif, tetapi penguasaan itu tidak otomatis disertai dengan kebiasaan mengamankan diri. Perilaku *oversharing*, yaitu dorongan untuk memperoleh validasi sosial, dan fenomena *Fear of Missing Out* (FOMO) mendorong mahasiswa membagikan informasi pribadi tanpa menimbang konsekuensinya, sehingga data yang seharusnya privat menjadi mudah dipanen pihak ketiga. Kebiasaan keamanan dasar pun masih lemah, misalnya penggunaan kata sandi yang berulang dan jarang diperbarui, serta minimnya penggunaan autentikasi dua faktor. Kondisi inilah yang penulis sebut sebagai paradoks digital, yaitu kemampuan memakai teknologi yang tinggi tetapi tidak diimbangi pemahaman untuk melindunginya.

Paradoks tersebut menegaskan bahwa akar kerentanan siber Generasi Z bersifat perilaku, bukan semata-mata karena teknis. Implikasinya, penguatan perangkat keamanan saja tidak akan menyelesaikan masalah apabila kebiasaan penggunanya tidak ikut dibenahi. Intervensi yang paling menentukan justru terletak pada edukasi dan pembentukan budaya sadar keamanan. Untuk mempertajam analisis ini, penulis memetakan dimensi-dimensi kerentanan siber Generasi Z beserta bentuk manifestasi dan implikasinya bagi keamanan kampus sebagaimana disajikan pada Tabel 1.

Tabel 1. Dimensi Kerentanan Siber Generasi Z di Lingkungan Perguruan Tinggi

No	Dimensi Kerentanan	Bentuk Manifestasi	Implikasi terhadap Keamanan Kampus
1	Kesenjangan literasi keamanan	Kemahiran teknis tinggi tetapi kesadaran mengamankan diri masih rendah	Pengguna menjadi titik terlemah meskipun sistem telah diperkuat
2	Perilaku *oversharing*	Kebiasaan membagikan data pribadi demi validasi sosial dan FOMO	Data sensitif mudah dipanen untuk rekayasa sosial dan pencurian identitas
3	Lemahnya kebiasaan dasar	Kata sandi berulang, jarang diperbarui, dan minim autentikasi dua faktor	Akun akademik rentan diambil alih dan disalahgunakan oleh pihak ketiga
4	Rendahnya persepsi ancaman	Ancaman siber dianggap tidak berdampak langsung pada diri sendiri	Motivasi untuk melindungi data melemah sehingga praktik keamanan sering diabaikan
5	Ketergantungan teknologi	Seluruh aktivitas akademik berlangsung di ruang digital	Permukaan serangan meluas dan dampak gangguan menjadi semakin besar

Tabel 1 memperlihatkan bahwa kemampuan menggunakan teknologi pada Generasi Z tidak berbanding lurus dengan kemampuan melindunginya. Pola yang konsisten muncul: intensitas digital yang tinggi berjalan beriringan dengan kesadaran keamanan yang rendah, dan kesenjangan itu menyempit secara nyata ketika edukasi keamanan diberikan secara terstruktur. Dengan demikian, literasi keamanan siber layak diposisikan sebagai variabel kunci sekaligus fondasi utama pertahanan siber di perguruan tinggi, sejajar dengan penguatan teknologi keamanannya.

Secara teoretis, paradoks digital ini dapat dipahami melalui *Protection Motivation Theory* yang menjelaskan bahwa seseorang baru terdorong melakukan tindakan perlindungan ketika ia memiliki persepsi ancaman yang tinggi sekaligus keyakinan bahwa tindakannya efektif. Pada Generasi Z, persepsi ancaman cenderung rendah karena ancaman siber sering tidak terasa langsung, sehingga motivasi untuk melindungi data pun melemah. Kerangka *Digital Native* memperkuat penjelasan ini: kedekatan sejak lahir dengan teknologi menumbuhkan rasa percaya diri yang berlebihan, padahal kefasihan menggunakan aplikasi berbeda dengan kecakapan menilai risiko keamanan. Penulis menilai bahwa kedua kerangka ini menegaskan satu hal yang sama, yaitu pembentukan kesadaran tidak dapat diserahkan pada proses alamiah, melainkan harus dirancang secara sengaja oleh institusi melalui edukasi yang terstruktur.

Lebih jauh, penulis memandang bahwa tanggung jawab membangun kesadaran ini tidak dapat dibebankan sepenuhnya kepada mahasiswa secara individual. Perguruan tinggi sebagai penyelenggara layanan digital juga memiliki kewajiban untuk menyediakan lingkungan yang aman sekaligus menumbuhkan kebiasaan digital yang sehat. Ketika kampus mendorong penggunaan teknologi untuk seluruh aktivitas akademik, kampus pula yang seharusnya menyiapkan bekal keamanan bagi penggunanya, mulai dari panduan praktis, pelatihan berkala, hingga keteladanan dalam pengelolaan data. Tanpa keterlibatan institusional yang aktif, paradoks digital akan terus berulang pada setiap angkatan mahasiswa baru karena kesadaran keamanan tidak terbentuk secara otomatis seiring meningkatnya kemahiran teknologi.

3.2 Pola Ancaman Siber yang Menyerang Lingkungan Perguruan Tinggi

Sebagai pengelola data strategis berupa identitas mahasiswa, data akademik, sistem keuangan, hingga hasil penelitian, kampus menjadi target bernilai tinggi bagi pelaku kejahatan siber. Penulis mengamati bahwa karakter ancaman terhadap perguruan tinggi telah bergeser dari bentuk yang sederhana menuju ancaman multidimensional. Ancaman tidak lagi

Jurnal Sains Dan Teknologi Informasi
Vol 5, No 3, Juni 2026, Hal 155-163
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v5i3.10311
Website https://ejurnal.seminar-id.com/index.php/jussi

terbatas pada peretasan sistem atau pencurian data, tetapi merambah manipulasi psikologis, propaganda digital, dan radikalisasi daring yang menyasar cara berpikir penggunanya.

Mahasiswa berada pada posisi paling rentan dalam peta ancaman ini. Penulis menilai bahwa sebagian besar mahasiswa belum mampu mengenali serangan *phishing* dan *malware* secara mandiri, sehingga mayoritas masih kesulitan membaca pola ancaman digital yang semakin terselubung. Kerentanan tersebut bukan sekadar potensi, melainkan telah terbukti dalam praktik: tercatat sejumlah kasus kebocoran data mahasiswa di perguruan tinggi nasional, bahkan ada data yang tersebar di *dark web*. Fakta ini menunjukkan bahwa percepatan transformasi digital kampus belum diiringi penguatan kesiapan keamanan yang setara, baik pada sisi sistem maupun pada sisi pengguna.

Di antara berbagai bentuk ancaman, *phishing* melalui media sosial merupakan yang paling dominan menyerang Generasi Z. Tingginya aktivitas pada platform seperti Instagram, TikTok, dan Twitter dimanfaatkan pelaku melalui tautan palsu, akun tiruan, promosi fiktif, dan pesan pribadi untuk memperoleh data sensitif. Yang menarik dari analisis penulis, persoalan utamanya bukan ketidaktahuan, melainkan kesenjangan antara kesadaran dan praktik: banyak mahasiswa memahami adanya ancaman, tetapi tidak menerapkan langkah perlindungan dalam keseharian. Pola ini menegaskan bahwa celah terbesar keamanan siber bukan pada sistem, melainkan pada faktor manusia, sebagaimana ditekankan dalam kerangka *Social Engineering Theory* yang menempatkan manipulasi kepercayaan pengguna sebagai pintu masuk utama serangan.

Ancaman pada perguruan tinggi juga berkembang ke ranah ideologis melalui *cyber radicalism*. Media sosial yang sama yang digunakan untuk belajar dan berinteraksi telah berubah menjadi ruang penyebaran narasi ekstrem, hoaks, dan propaganda yang menyasar Generasi Z. Penulis berpendapat bahwa kerentanan terhadap ancaman ini berakar pada lemahnya kemampuan berpikir kritis dan rendahnya literasi digital, yang membuat informasi provokatif mudah diterima tanpa verifikasi. Dalam konteks kampus, ancaman semacam ini berbahaya karena tidak hanya mengincar data, tetapi juga berpotensi mengganggu stabilitas akademik dan membentuk polarisasi di kalangan mahasiswa. Kompleksitas tersebut menempatkan keamanan siber sebagai persoalan lintas sektor yang menuntut kolaborasi, kepemimpinan digital, dan penguatan kesadaran kolektif, bukan sekadar penguatan perangkat. Kerangka *Risk Society* dari Ulrich Beck relevan untuk menjelaskan ironi ini: modernisasi yang menghadirkan kemudahan justru melahirkan bentuk risiko baru yang harus dikelola secara sadar dan berkelanjutan. Untuk merangkum analisis ini, penulis memetakan pola ancaman siber yang dominan beserta sasaran utama dan strategi pertahanan yang relevan sebagaimana disajikan pada Tabel 2.

Tabel 2. Pemetaan Pola Ancaman Siber dan Strategi Pertahanan Berlapis pada Perguruan Tinggi

No	Jenis Ancaman	Sasaran Utama	Strategi Pertahanan
1	*Phishing* dan rekayasa sosial	Kredensial dan data pribadi mahasiswa	Edukasi pengenalan tautan palsu serta verifikasi sumber dan pengirim
2	*Malware* dan peretasan sistem	Basis data akademik dan sistem keuangan kampus	Enkripsi data, pembaruan sistem berkala, dan mekanisme pencadangan
3	Pencurian dan kebocoran data	Identitas sivitas akademika dan arsip penelitian	Tata kelola data yang ketat dan prosedur tanggap insiden
4	*Cyber radicalism* dan propaganda	Pola pikir dan ketahanan ideologis mahasiswa	Penguatan literasi digital dan kemampuan berpikir kritis
5	Disinformasi dan hoaks	Stabilitas akademik dan reputasi institusi	Budaya verifikasi informasi dan penguatan kanal komunikasi resmi

Tabel 2 menunjukkan bahwa ancaman siber pada perguruan tinggi telah bergeser dari persoalan teknis menjadi persoalan sosial dan kultural. Ancaman tidak hanya menyerang sistem, tetapi juga menyasar pola pikir, perilaku, dan ketahanan ideologis mahasiswa, sehingga setiap jenis ancaman menuntut strategi pertahanan yang berbeda namun saling melengkapi. Konsekuensinya, model pertahanan siber kampus yang efektif tidak dapat dibangun pada satu lapis saja, melainkan harus berlapis dan saling menopang.

Pemetaan pada Tabel 2 pada dasarnya merupakan penerapan metode *Defense-in-Depth* (Gambar 1) dalam menyelesaikan masalah keamanan siber Generasi Z. Pada lapisan manusia, penguatan literasi dan edukasi digital menekan keberhasilan rekayasa sosial dan *phishing* yang menjadikan perilaku pengguna sebagai titik terlemah; pada lapisan teknologi, penerapan autentikasi multifaktor, enkripsi, dan pemantauan jaringan menutup celah teknis seperti pencurian kredensial dan kebocoran data; sedangkan pada lapisan operasi dan kebijakan, tata kelola, regulasi, serta prosedur respons insiden memastikan ancaman tertangani secara terstruktur dan berkelanjutan. Dengan demikian, setiap lapisan saling melengkapi sehingga kegagalan pada satu kontrol tidak serta-merta membahayakan aset inti perguruan tinggi.

Dampak ancaman siber pada perguruan tinggi juga tidak berhenti pada kerugian individual mahasiswa. Kebocoran data akademik dapat menurunkan kepercayaan publik terhadap institusi, mengganggu kelangsungan layanan pembelajaran, dan merusak reputasi yang dibangun selama bertahun-tahun. Pada serangan yang melumpuhkan sistem, aktivitas akademik seperti perkuliahan daring, ujian, dan pengelolaan nilai dapat terhenti sehingga merugikan banyak pihak sekaligus. Penulis menilai bahwa skala dampak inilah yang menempatkan keamanan siber bukan sebagai urusan teknis unit teknologi informasi semata, melainkan sebagai isu strategis yang menyentuh keberlangsungan dan kredibilitas institusi pendidikan tinggi secara keseluruhan.

Jurnal Sains Dan Teknologi Informasi
Vol 5, No 3, Juni 2026, Hal 155-163
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v5i3.10311
Website https://ejurnal.seminar-id.com/index.php/jussi

Hal lain yang perlu digarisbawahi adalah adanya kesenjangan antara pengetahuan dan tindakan. Mahasiswa pada umumnya mengetahui bahwa tautan mencurigakan berbahaya, bahwa kata sandi perlu kuat, dan bahwa data pribadi tidak boleh disebarkan sembarangan; namun pengetahuan tersebut tidak selalu berubah menjadi kebiasaan. Penulis menilai kesenjangan inilah yang menjadi sasaran utama pelaku kejahatan siber, sebab serangan modern dirancang untuk mengeksploitasi kelengahan dan kebiasaan, bukan semata kelemahan sistem. Oleh karena itu, ukuran keberhasilan pertahanan siber kampus tidak cukup dilihat dari tersedianya teknologi keamanan, melainkan dari sejauh mana perilaku aman benar-benar dipraktikkan oleh seluruh sivitas akademika secara konsisten.

Berangkat dari temuan tersebut, penulis merumuskan kerangka pertahanan siber kampus yang terdiri atas tiga lapis. Lapis teknologi mencakup penguatan infrastruktur seperti enkripsi data, autentikasi berlapis, pembaruan sistem secara berkala, dan mekanisme pencadangan untuk meminimalkan dampak serangan. Lapis kebijakan mencakup tata kelola data, prosedur tanggap insiden, serta aturan penggunaan layanan digital kampus yang jelas dan ditegakkan. Lapis manusia, yang merupakan lapis paling menentukan, mencakup edukasi keamanan siber berkelanjutan, pembentukan budaya sadar keamanan, dan penguatan kemampuan berpikir kritis mahasiswa. Ketiga lapis ini harus berjalan serentak, sebab kekuatan teknologi akan sia-sia bila pengguna tetap menjadi titik lemah, dan sebaliknya, kesadaran pengguna membutuhkan dukungan sistem dan kebijakan yang memadai. Penulis menegaskan bahwa keunggulan kerangka berlapis ini terletak pada sifatnya yang saling mengompensasi: ketika satu lapis melemah, lapis lainnya masih mampu menahan laju serangan sehingga dampaknya dapat diminimalkan. Dengan kerangka inilah perguruan tinggi dapat menghadapi ancaman siber yang terus berevolusi secara lebih adaptif dan berkelanjutan.

Implikasi dari kerangka berlapis tersebut bersifat praktis sekaligus strategis. Secara praktis, perguruan tinggi perlu menempatkan edukasi keamanan siber sebagai bagian integral dari layanan akademik, misalnya melalui pelatihan pengenalan *phishing* secara berkala, kampanye kesadaran keamanan digital, serta penyediaan panduan penggunaan kata sandi yang kuat dan autentikasi dua faktor. Secara kelembagaan, kampus dituntut membangun tata kelola data yang jelas, menetapkan prosedur tanggap insiden, dan memperlakukan keamanan siber sebagai indikator mutu layanan digital, bukan sekadar urusan teknis satu unit kerja. Penulis memandang bahwa keterpaduan ketiga lapis ini hanya akan berjalan apabila pimpinan institusi menempatkan keamanan siber sebagai prioritas kebijakan sekaligus melibatkan seluruh sivitas akademika dalam pelaksanaannya secara konsisten.

Sintesis atas seluruh temuan ini sekaligus menjawab ketiga tujuan penelitian. Pertama, sistem pertahanan siber perguruan tinggi yang selama ini berfokus pada penguatan aspek teknis terbukti belum memadai karena mengabaikan dimensi perilaku pengguna sebagai titik terlemah. Kedua, *phishing*, pencurian data pribadi, *social engineering*, dan *cyber radicalism* teridentifikasi sebagai bentuk ancaman digital yang paling dominan menyerang mahasiswa Generasi Z. Ketiga, arah penguatan yang paling menentukan terletak pada peningkatan literasi digital dan kesadaran keamanan yang berfungsi sebagai fondasi bagi terbentuknya pertahanan siber kampus yang adaptif, preventif, dan berkelanjutan. Dengan demikian, pergeseran fokus dari pendekatan teknis semata menuju pendekatan yang menempatkan manusia sebagai inti pertahanan menjadi kontribusi utama yang ditawarkan penelitian ini bagi pengelolaan keamanan siber di lingkungan pendidikan tinggi.

3.3 Pembahasan

Untuk menegaskan posisi dan kontribusi penelitian ini, temuan yang diperoleh perlu didiskusikan secara komparatif dengan hasil penelitian terdahulu. Pembahasan ini diarahkan untuk memperlihatkan letak persamaan, perbedaan, sekaligus pengembangan yang ditawarkan penelitian ini terhadap kajian-kajian sebelumnya seputar keamanan siber, literasi digital, dan perilaku digital Generasi Z, sehingga kebaruan yang diklaim dapat diuji secara terbuka terhadap bukti yang telah ada.

Temuan pertama penelitian ini menunjukkan bahwa akar kerentanan siber Generasi Z bersifat perilaku, yaitu paradoks digital berupa tingginya kemahiran teknologi yang tidak diimbangi kesadaran keamanan. Temuan ini sejalan dengan penelitian Budiman dkk. [14] yang menyimpulkan bahwa perilaku konsumtif Generasi Z dalam ekonomi digital belum dibarengi kesadaran keamanan yang memadai, serta dengan kajian Nopriadi [15] yang menemukan bahwa dorongan memperoleh validasi sosial mendorong perilaku berbagi data pribadi sehingga meningkatkan risiko pencurian identitas. Perbedaannya, kedua penelitian tersebut menyoroti perilaku digital pada konteks ekonomi dan media sosial secara umum, sedangkan penelitian ini menempatkan paradoks digital tersebut secara spesifik sebagai titik terlemah dalam sistem pertahanan siber perguruan tinggi.

Temuan kedua, yaitu dominasi *phishing*, pencurian data pribadi, *social engineering*, dan *cyber radicalism* sebagai ancaman utama, memperkuat sekaligus memperluas hasil penelitian terdahulu. Tan dkk. [18] menemukan bahwa sebagian besar mahasiswa belum mampu mengenali serangan siber secara mandiri, dan penelitian ini mempertegas temuan tersebut melalui data bahwa hanya sekitar 40% mahasiswa yang mampu mengenali ancaman *phishing* secara mandiri. Putri dkk. [19] menunjukkan bahwa *phishing* memanfaatkan tingginya penggunaan media sosial mahasiswa, sementara Arianti dkk. [20] menyoroti berkembangnya *cyber radicalism* yang menyebarkan propaganda melalui media sosial untuk menyasar Generasi Z. Penelitian ini mengintegrasikan kedua jenis ancaman tersebut, baik yang bersifat teknis maupun ideologis, ke dalam satu peta ancaman sehingga memberikan gambaran yang lebih utuh dibanding penelitian sebelumnya yang umumnya membahas masing-masing ancaman secara terpisah.

Temuan ketiga berkaitan dengan efektivitas edukasi keamanan siber. Hasil penelitian ini menegaskan bahwa edukasi yang terstruktur meningkatkan pemahaman keamanan digital, dengan kenaikan pengetahuan keamanan data

Jurnal Sains Dan Teknologi Informasi
Vol 5, No 3, Juni 2026, Hal 155-163
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v5i3.10311
Website https://ejurnal.seminar-id.com/index.php/jussi

sebesar 8,33 poin dan pemahaman risiko teknologi sebesar 10,17 poin. Temuan ini konsisten dengan kajian Prümmer dkk. [16] yang menyimpulkan bahwa metode pelatihan keamanan siber yang terstruktur efektif meningkatkan pengetahuan dan kewaspadaan pengguna, serta dengan Surbakti [2] yang menekankan pentingnya edukasi untuk berdigital secara aman. Akan tetapi, penelitian ini memberikan kontribusi tambahan dengan menempatkan edukasi tersebut sebagai bagian dari lapisan manusia (*people*) dalam kerangka pertahanan berlapis *Defense-in-Depth*, bukan sebagai intervensi yang berdiri sendiri.

Dari sisi strategi pertahanan, penelitian terdahulu cenderung menyoroti aspek tertentu secara parsial. Suryati dkk. [12] menekankan pendekatan berbasis komunitas untuk mengubah generasi muda menjadi pelindung keamanan siber yang aktif, sedangkan Nasoha dkk. [13] menyoroti penguatan kapasitas sumber daya manusia dan kepemimpinan digital. Kajian kebijakan keamanan siber nasional [17], umumnya membahas keamanan siber pada tataran regulasi dan tata kelola negara. Penelitian ini berbeda karena memadukan ketiga dimensi tersebut, yakni manusia, teknologi, serta operasi dan kebijakan, ke dalam satu kerangka metode *Defense-in-Depth* yang diterapkan khusus pada konteks perguruan tinggi dengan Generasi Z sebagai variabel utama. Dengan demikian, kebaruan penelitian ini terletak pada upayanya untuk menjembatani aspek teknis pertahanan siber dengan aspek perilaku dan literasi digital mahasiswa dalam satu kerangka analisis yang utuh, sebuah integrasi yang belum dilakukan secara eksplisit oleh penelitian-penelitian sebelumnya.

Berdasarkan perbandingan tersebut, penelitian ini tidak hanya mengonfirmasi temuan terdahulu mengenai rendahnya literasi keamanan dan tingginya kerentanan Generasi Z, tetapi juga memberikan kontribusi baru berupa model pertahanan siber kampus berlapis yang menempatkan manusia sebagai inti pertahanan. Posisi ini sekaligus menjawab kesenjangan penelitian (*research gap*) yang telah diidentifikasi pada bagian pendahuluan, yaitu masih terbatasnya kajian yang mengintegrasikan karakteristik perilaku digital Generasi Z ke dalam sistem pertahanan siber institusi pendidikan tinggi.

4. KESIMPULAN

Berdasarkan analisis terhadap beragam literatur, penelitian ini menyimpulkan bahwa kerentanan siber pada perguruan tinggi berakar pada faktor perilaku Generasi Z, yaitu paradoks digital berupa kemahiran teknologi yang tinggi tetapi tidak diimbangi literasi dan kesadaran keamanan yang memadai, sehingga *phishing*, pencurian data pribadi, *social engineering*, dan *cyber radicalism* menjadi ancaman yang paling dominan di lingkungan kampus. Ancaman tersebut terbukti tidak lagi bersifat teknis semata, melainkan telah berkembang menjadi ancaman multidimensional yang menyasar pola pikir, perilaku sosial, dan ketahanan ideologis mahasiswa melalui media sosial. Oleh karena itu, pertahanan siber perguruan tinggi yang efektif menuntut model berlapis yang memadukan penguatan teknologi, ketegasan kebijakan tata kelola data, dan yang paling menentukan adalah penguatan literasi serta budaya sadar keamanan pada seluruh sivitas akademika, dengan literasi digital sebagai fondasi utamanya. Penelitian ini menegaskan bahwa keberhasilan pertahanan siber kampus tidak cukup diukur dari kecanggihan perangkat, tetapi dari sejauh mana perilaku aman dipraktikkan secara konsisten oleh setiap individu. Secara praktis, perguruan tinggi disarankan menjadikan edukasi dan budaya sadar keamanan siber sebagai bagian integral dari strategi institusi serta membangun kolaborasi dengan pemerintah dan komunitas keamanan siber, sementara bagi penelitian selanjutnya diperlukan studi lapangan atau pendekatan kuantitatif untuk mengukur secara empiris efektivitas model pertahanan siber berbasis literasi digital pada perguruan tinggi di Indonesia, sekaligus menguji penerapan kerangka pertahanan berlapis ini pada konteks kampus yang lebih beragam agar temuannya dapat digeneralisasi secara lebih luas.

REFERENCES

[1] D. Prasetyo, E. A. Hualakhi, N. Ramadhani, and K. K. Wardani, "Perancangan Animasi Edukatif Keamanan Siber Berbasis Storytelling untuk Generasi Z," *J. Desain*, vol. 13, no. 3, pp. 802–811, 2026, doi: 10.30998/jd.v13i3.2120.

[2] F. P. S. Surbakti, "Edukasi Keamanan Siber Berdigital dengan Aman," *Prima Abdika J. Pengabdi. Masy.*, vol. 4, no. 4, pp. 868–878, 2024, doi: 10.37478/abdika.v4i4.4967.

[3] T. W. Ramadhan and D. Permadi, "Analisis Framing Pemberitaan Peretasan Pusat Data Nasional (PDN) di Media Online Tempo.co," *J. Educ. Res.*, vol. 5, no. 3, pp. 3368–3379, 2024, doi: 10.37985/jer.v5i3.1491.

[4] I. Aryasatya, S. Riyanta, and E. Daryanto, "Jurnal Impresi Indonesia (JII) Analisis Kebijakan Keamanan Siber Indonesia dalam Strategi Nasional Keamanan Siber," vol. 5, no. 3, pp. 1411–1427, 2026.

[5] V. Kusumawardani, D. A. C. Agustin, and S. S. Permatasari, "Social Media and Political Preferences among Generation Z in the 2024 Indonesian Presidential Election," *Mediakita*, vol. 9, no. 2, pp. 246–269, 2025, doi: 10.30762/mediakita.v9i2.2762.

[6] H. Harmen, A. N. S. B. D. Dalimunthe, D. I. Lestari, F. Al Kautsar, J. S. Sihombing, and T. C. B. S. Simanjuntak, "Strategi Penguatan Keamanan Informasi Digital dalam Menghadapi Ancaman Siber: Studi Kasus Kementerian Kominfo," *EKOMA J. Ekon. Manajemen, Akunt.*, vol. 4, no. 6, pp. 8541–8550, 2025, doi: 10.56799/ekoma.v4i6.9870.

[7] R. Wijaya and D. Juardi, "Edukasi Masyarakat tentang Keamanan Siber dalam Tantangan dan Solusi di Era Digital," *J. Inform. dan Tek. Elektro Terap.*, vol. 14, no. 1, 2026, doi: 10.23960/jitet.v14i1.8336.

[8] V. C. Febriana and R. Indrarini, "Pengaruh Cyber Crime dan Cyber Security terhadap Tingkat Kepercayaan Nasabah Bank Syariah dalam Menggunakan Layanan M-Banking di Wilayah Surabaya," *JEKoBi J. Ekon. dan Bisnis*, vol. 7, no. 3, pp. 161–174, 2024, doi: 10.26740/jekobi.v7n3.p161-174.

[9] J. Triyanto, Sunardi, and I. Riadi, "Analisis Investigasi Cyber Espionage pada Facebook Menggunakan Digital Forensics Research Workshop (DFRWS)," *Techno J. Fak. Tek. Univ. Muhammadiyah Purwokerto*, vol. 23, no. 1, pp. 39–46, 2022, doi:

Vol 5, No 3, Juni 2026, Hal 155-163
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v5i3.10311
Website https://ejurnal.seminar-id.com/index.php/jussi

10.30595/techno.v23i1.9064.
[10] M. Alfian and R. Rahman, "Keamanan Jaringan pada Perguruan Tinggi," *J. Ris. Sist. Inf.*, vol. 1, no. 3, pp. 59–64, 2024, doi: 10.69714/qgnbgv11.
[11] R. Okra and A. Abdussalam, "Peran Literasi Digital dalam Mencegah Penyalahgunaan Data Pribadi Generasi Z di Kota Mataram," *J. Sist. Inf. dan Teknol. Era*, vol. 1, no. 1, pp. 12–19, 2025, doi: 10.71094/sitera.v1i1.47.
[12] S. Suryati, L. Sardana, R. Disurya, and Y. S. Putra, "Penguatan Literasi Digital dalam Pencegahan Pelanggaran Hukum Siber (Cyber Law)," *Wajah Huk.*, vol. 8, no. 1, pp. 84–94, 2024, doi: 10.33087/wjh.v8i1.1447.
[13] A. M. M. Nasoha, A. N. Atqiya, T. N. Ramadani, W. N. Hidayah, and E. S. Nasicha, "Peran Kewarganegaraan Digital dalam Perspektif Hukum Islam bagi Muslim di Dunia Maya," *Konsensus J. Ilmu Pertahanan, Huk. dan Ilmu Komun.*, vol. 2, no. 2, pp. 134–144, 2025, doi: 10.62383/konsensus.v2i2.742.
[14] D. Budiman, Y. Sutrasna, and Sakum, "Perilaku Konsumtif Gen Z dan Kesadaran Keamanan Digital dalam Ekonomi Digital Indonesia," *JUMINTAL J. Manaj. Inform. dan Bisnis Digit.*, vol. 4, no. 2, pp. 317–328, 2025, doi: 10.55123/jumintal.v4i2.6776.
[15] Nopriadi, "Menjaga Privasi Digital: Studi tentang Kesadaran Mahasiswa dalam Perlindungan Data Pribadi di Media Sosial," *Polyg. J. Ilmu Komput. dan Ilmu Pengetah. Alam*, vol. 3, no. 3, pp. 42–52, 2025, doi: 10.62383/polygon.v2i6.297.
[16] J. Prümmer, T. van Steen, and B. van den Berg, "A Systematic Review of Current Cybersecurity Training Methods," *Comput. Secur.*, vol. 136, p. 103585, 2024, doi: 10.1016/j.cose.2023.103585.
[17] I. T. Bua and N. I. Idris, "Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024," *Desentralisasi J. Hukum, Kebijak. Publik, dan Pemerintah.*, vol. 2, no. 2, pp. 100–114, 2025, doi: 10.62383/desentralisasi.v2i2.653.
[18] T. Tan, H. Sama, T. Wibowo, G. Wijaya, and O. E. Aboagye, "Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam," *J. Teknol. dan Inf.*, vol. 14, no. 2, pp. 163–173, 2024, doi: 10.34010/jati.v14i2.12518.
[19] A. Putri, N. Sari, P. Fajrina, and S. Aisyah, "Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital," *J. Pengabdi. Nas. Indones.*, vol. 6, no. 1, pp. 38–52, 2025, doi: 10.35870/jpni.v6i1.1097.
[20] A. Arianti *et al.*, "Peran Pendidikan Kewarganegaraan dalam Mencegah Radikalisme di Kalangan Remaja Gen Z," *Katalis Pendidik. J. Ilmu Pendidik. dan Mat.*, vol. 1, no. 3, pp. 226–232, 2024, doi: 10.62383/katalis.v1i3.592.
[21] M. Tahmasebi, "Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises," *J. Inf. Secur.*, vol. 15, no. 2, pp. 106–133, 2024, doi: 10.4236/jis.2024.152008.
[22] J. N. Al-Karaki and H. M. Zangana, "Defense in Depth: A Multilayered Approach," in *Defense in Depth*, Hoboken, NJ: Wiley, 2025. doi: 10.1002/9781394340750.ch3.