ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 29856-29866
Volume 8 Nomor 2 Tahun 2024

Pengaruh Ancaman Siber terhadap Operasi Keamanan Laut TNI Al dan Upaya Mitigasi melalui Edukasi Media Sosial

Toni Hermawan[1], Muhammad Zulkifli[2], Manahan Budiarto Pandjaitan[3]

[1,2,3] Sekolah Staff dan Komando TNI Angkatan Laut

e-mail: toni.hermawan@icloud.com

Abstrak

Dalam era digital yang semakin maju, ancaman siber menjadi salah satu tantangan terbesar bagi keamanan nasional, termasuk bagi TNI Angkatan Laut (TNI AL) Indonesia. Ancaman ini tidak hanya menyasar infrastruktur fisik, tetapi juga mengincar sistem digital dan informasi yang digunakan dalam operasi militer. Penelitian ini bertujuan untuk menganalisis pengaruh tingkat pendidikan dan lama pengabdian terhadap pemahaman dan kewaspadaan personel TNI AL terhadap ancaman siber. Penelitian ini menggunakan pendekatan kuantitatif dengan alat analisis statistik SPSS. Data dikumpulkan melalui survei terstruktur yang disebarkan kepada 60 personel TNI AL yang terlibat langsung dalam operasi keamanan laut. Survei ini dirancang untuk mengukur tingkat pendidikan, lama pengabdian, serta pemahaman dan kewaspadaan mereka terhadap ancaman siber. Analisis data mencakup uji statistik deskriptif, uji normalitas, dan uji t untuk signifikansi parameter individual. Hasil penelitian menunjukkan bahwa tingkat pendidikan rata-rata personel adalah 62.05 (skala 100) dengan deviasi standar 7.55, dan lama pengabdian rata-rata adalah 99.07 tahun dengan deviasi standar 12.30. Pemahaman dan kewaspadaan terhadap ancaman siber memiliki rata-rata 82.95 dengan deviasi standar 10.24. Uji t mengindikasikan bahwa tingkat pendidikan memiliki koefisien tidak terstandarisasi sebesar 0.408 dengan nilai t sebesar 2.377 dan nilai Sig. sebesar 0.021, menunjukkan pengaruh signifikan terhadap pemahaman dan kewaspadaan terhadap ancaman siber. Lama pengabdian juga memiliki pengaruh yang sangat signifikan dengan koefisien tidak terstandarisasi sebesar 0.003, nilai t sebesar 14.376, dan nilai Sig. sebesar 0.000.

Kata Kunci: *Ancaman Siber, TNI Angkatan Laut (TNI AL), Keamanan Laut, Tingkat Pendidikan, Lama Pengabdian*

Abstract

In the increasingly advanced digital era, cyber threats are one of the biggest challenges for national security, including for the Indonesian Navy (TNI AL). This threat not only targets physical infrastructure, but also targets digital and information systems used in military operations. This research aims to analyze the influence of education level and length of service on the understanding and awareness of Indonesian Navy personnel towards cyber threats. This research uses a quantitative approach with the SPSS statistical analysis tool. Data was collected through a structured survey distributed to 60 Indonesian Navy personnel who were directly involved in maritime security operations. This survey was designed to measure their level of education, length of service, as well as their understanding and awareness of cyber threats. Data analysis includes descriptive statistical tests, normality tests, and t tests for the significance of individual parameters. The research results show that the average education level of personnel is 62.05 (scale 100) with a standard deviation of 7.55, and the average length of service is 99.07 years with a standard deviation of 12.30. Understanding and awareness of cyber threats has an average of 82.95 with a standard deviation of 10.24. The t test indicates that the level of education has a non-standardized coefficient of 0.408 with a t value of 2.377 and a Sig. of 0.021, indicating a significant

influence on understanding and awareness of cyber threats. Length of service also has a very significant influence with a non-standardized coefficient of 0.003, a t value of 14.376, and a Sig value. of 0,000.

Keywords: *Cyber Threats, Indonesian Navy (TNI AL), Maritime Security, Education Level, Length of Service*

PENDAHULUAN

Ancaman siber terhadap operasi keamanan laut TNI AL menjadi perhatian utama dalam pertahanan nasional Indonesia di era digital ini. Sebagai salah satu cabang utama dari Tentara Nasional Indonesia, TNI AL memiliki peran krusial dalam menjaga kedaulatan maritim, melindungi perairan Indonesia, serta mengamankan jalur pelayaran vital bagi perekonomian dan keamanan negara (Babys, 2021). Namun, dengan semakin kompleksnya teknologi yang digunakan dalam operasi militer modern, keberadaan ancaman siber menghadirkan tantangan baru yang signifikan (Alfi et al., 2023).

Ancaman siber dapat berdampak langsung terhadap berbagai aspek operasional TNI AL. Salah satu dampak utama adalah pada sistem komunikasi mereka. Komunikasi yang handal dan aman adalah kunci utama dalam kesuksesan setiap operasi militer. Ancaman siber bisa menyebabkan gangguan atau bahkan pemutusan komunikasi antara kapal-kapal, pangkalan, dan markas TNI AL. Serangan yang mengganggu frekuensi radio atau mengacaukan sistem satelit dapat menghambat koordinasi operasional yang efektif, serta memperlambat respon terhadap situasi darurat di laut (Soesanto et al., 2023).

Tak hanya itu, ancaman siber juga dapat mengintai pada sistem navigasi kapal-kapal perang TNI AL. Sistem GPS dan navigasi yang digunakan untuk memandu kapal-kapal dapat menjadi target manipulasi atau penyusupan oleh pihak yang tidak bertanggung jawab. Manipulasi terhadap sistem navigasi ini bukan hanya meningkatkan risiko kecelakaan di laut, tetapi juga dapat memungkinkan musuh untuk melacak gerakan dan posisi kapal-kapal TNI AL dengan lebih mudah, membuka peluang untuk serangan yang lebih efektif (Lana, 2021).

Keamanan data dan informasi rahasia merupakan hal lain yang menjadi perhatian serius dalam ancaman siber terhadap TNI AL. Informasi strategis seperti rencana operasi, posisi kapal-kapal, dan strategi pertahanan nasional dapat menjadi target empuk bagi serangan siber. Pencurian data atau akses ilegal ke informasi rahasia ini tidak hanya mengancam keamanan nasional, tetapi juga dapat mempengaruhi kesiapan dan strategi pertahanan negara secara keseluruhan. Perlindungan data dan sistem informasi militer menjadi sangat penting dalam menghadapi ancaman ini (Narindra, 2021).

Selain itu, gangguan pada sistem-sistem elektronik yang mengendalikan senjata, pengawasan, dan peralatan lainnya juga merupakan risiko nyata akibat ancaman siber. Serangan yang menyasar sistem pengawasan radar atau mencoba mengakses sistem kendali senjata dapat mengganggu fungsi operasional TNI AL secara signifikan. Kerusakan fisik pada peralatan militer atau gangguan terhadap sistem pengawasan bisa membuka celah bagi kelemahan yang dapat dimanfaatkan oleh pihak musuh (Benyamin et al., 2023).

Untuk mengatasi kompleksitas ancaman siber terhadap operasi keamanan laut TNI AL, diperlukan pendekatan mitigasi yang holistik dan terintegrasi. Salah satu langkah krusial adalah penerapan kebijakan keamanan cyber yang ketat. Hal ini meliputi penggunaan sandi yang kuat, enkripsi data, serta penerapan protokol keamanan yang mutakhir di seluruh sistem-sistem militer TNI AL. Di Indonesia, kerangka hukum terkait keamanan cyber telah berkembang dengan signifikan, mencakup Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang memberikan landasan hukum untuk penanganan kejahatan siber termasuk serangan terhadap sistem komputer (Astarini & Rofii, 2021).

Pendidikan dan pelatihan juga memegang peran penting dalam membangun pertahanan cyber yang kuat. Personel TNI AL perlu dilengkapi dengan pengetahuan dan keterampilan yang diperlukan untuk mengenali, melaporkan, dan merespons ancaman siber dengan tepat waktu. Pelatihan ini harus mencakup pengenalan terhadap jenis-jenis

serangan cyber, taktik yang digunakan oleh penyerang, serta praktik keamanan cyber yang dapat diterapkan dalam operasi sehari-hari (Samad & Persadha, 2022).

Pengembangan kemampuan teknologi cyber juga menjadi fokus utama dalam menghadapi ancaman siber. Investasi dalam sistem pengawasan jaringan, deteksi dini terhadap serangan, dan respons cepat terhadap insiden menjadi kunci dalam menjaga keamanan sistem-sistem militer. Teknologi kecerdasan buatan (AI) dan analisis data juga dapat dimanfaatkan untuk meningkatkan kemampuan dalam memprediksi dan mencegah serangan siber sebelum mereka menyebabkan kerusakan yang signifikan (Afiansyah & Febriyani, 2023). Selain itu, kerjasama internasional dalam hal pertukaran informasi mengenai ancaman siber dan praktik terbaik dalam keamanan cyber juga menjadi penting. Indonesia perlu aktif berpartisipasi dalam forum internasional untuk memperkuat kerjasama lintas batas dalam menghadapi ancaman siber yang semakin kompleks dan meluas (Benyamin et al., 2023).

Edukasi melalui media sosial memiliki peran yang krusial dalam mendukung strategi mitigasi ancaman siber. Media sosial tidak hanya sebagai alat untuk berbagi informasi, tetapi juga sebagai platform untuk meningkatkan kesadaran dan keterampilan keamanan cyber di kalangan personel TNI AL (Susanto et al., 2023). Kampanye kesadaran cyber, pelatihan online, forum diskusi, dan webinar dapat digunakan untuk menyebarkan informasi tentang ancaman siber terbaru, praktik keamanan cyber yang aman, serta studi kasus untuk memperkuat pemahaman dan kesiapan personel (Rahmawati, 2020). Menghadapi ancaman siber terhadap operasi keamanan laut TNI AL membutuhkan pendekatan yang komprehensif dan kolaboratif dari berbagai pihak terkait. Perlindungan terhadap infrastruktur informasi militer, peningkatan keterampilan dan kesadaran personel, serta investasi dalam teknologi dan kerjasama internasional adalah kunci untuk membangun pertahanan cyber yang kokoh dan efektif (Budi et al., 2021). Dengan demikian, TNI AL dapat memastikan bahwa operasi-operasi keamanan lautnya tetap efektif dan mampu menjaga kedaulatan serta keamanan nasional Indonesia di era digital yang terus berkembang ini.

Permasalahan yang dihadapi oleh TNI AL dalam keamanan cyber adalah meningkatnya ancaman siber yang dapat mengganggu operasi keamanan laut mereka. Seiring dengan kemajuan teknologi informasi dan ketergantungan pada sistem-sistem digital, TNI AL menghadapi tantangan kompleks dalam melindungi infrastruktur, data sensitif, dan komunikasi mereka dari serangan cyber yang semakin canggih dan beragam. Ancaman ini tidak hanya mencakup potensi gangguan terhadap sistem komunikasi dan navigasi, tetapi juga risiko terhadap keamanan data dan informasi strategis militer yang dapat dieksploitasi oleh pihak asing atau kelompok yang tidak bertanggung jawab.

Tujuan utama dari penelitian ini adalah untuk mengidentifikasi dan menganalisis strategi mitigasi yang efektif terhadap ancaman siber terhadap operasi keamanan laut TNI AL. TNI AL dapat memperkuat pertahanan cyber mereka melalui kebijakan keamanan yang tepat, pelatihan dan pendidikan yang intensif bagi personel, pengembangan teknologi cyber yang canggih, serta kerjasama internasional yang erat dalam menghadapi ancaman cyber lintas batas.

Gap dalam penelitian saat ini terletak pada kurangnya fokus yang memadai pada aspek keamanan cyber dalam militer, khususnya dalam operasi keamanan laut TNI AL. Studi-studi yang mendalam mengenai ancaman siber terhadap sistem komunikasi dan navigasi TNI AL, serta pengembangan strategi mitigasi yang spesifik untuk situasi ini masih terbatas. Selain itu, kurangnya data empiris yang menyediakan pemahaman mendalam tentang dampak konkret dari serangan siber terhadap operasional militer juga menjadi kekurangan yang perlu diisi.

Urgensi dari penelitian ini sangatlah penting mengingat eskalasi ancaman siber yang terus meningkat dan potensi dampak yang dapat merusak dalam operasi militer TNI AL. Keamanan cyber bukan hanya masalah teknis semata, tetapi juga memiliki implikasi strategis yang dapat mempengaruhi kemampuan pertahanan dan keamanan nasional secara keseluruhan. Dengan memahami urgensi ancaman ini secara lebih mendalam, TNI

AL dapat mengambil langkah-langkah proaktif untuk meningkatkan keamanan sistem-sistem kritis mereka dan meminimalkan kerentanan terhadap serangan siber yang dapat merugikan.

Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam mengisi kesenjangan pengetahuan yang ada, menyediakan rekomendasi konkret untuk kebijakan dan strategi mitigasi, serta memperkuat kesiapan TNI AL dalam menghadapi ancaman siber di masa depan. Langkah-langkah ini penting untuk memastikan bahwa operasi keamanan laut TNI AL tetap efektif, aman, dan mampu menjaga kedaulatan maritim serta keamanan nasional Indonesia secara keseluruhan.

METODE

Penelitian ini menggunakan pendekatan kuantitatif dengan menggunakan alat analisis statistik SPSS. Pendekatan ini dipilih untuk memungkinkan pengumpulan data yang sistematis dan obyektif mengenai ancaman siber terhadap operasi keamanan laut TNI AL. Metode pengumpulan data dilakukan melalui survei terstruktur yang disebarkan kepada personel TNI AL yang terlibat langsung dalam operasi keamanan laut. Survei ini dirancang untuk mengumpulkan informasi tentang tingkat pemahaman mereka terhadap ancaman siber, pengalaman mereka dalam menghadapi serangan cyber, serta persepsi mereka terhadap efektivitas kebijakan keamanan cyber yang diterapkan.

Data yang terkumpul akan dianalisis menggunakan perangkat lunak statistik SPSS (Statistical Package for the Social Sciences) untuk melakukan analisis deskriptif dan inferensial. Analisis deskriptif akan digunakan untuk merumuskan gambaran umum mengenai tingkat ancaman siber yang dihadapi TNI AL, sementara analisis inferensial akan digunakan untuk menguji hubungan antara variabel-variabel tertentu, seperti tingkat pendidikan personel dengan tingkat pemahaman mereka terhadap ancaman siber.

Selain survei, penelitian ini juga akan memanfaatkan tinjauan pustaka yang komprehensif untuk mendapatkan pemahaman mendalam tentang teori-teori dan penelitian terkait dalam domain keamanan cyber militer. Tinjauan pustaka ini akan mencakup studi-studi kasus tentang serangan siber terhadap militer di berbagai negara, strategi mitigasi yang telah terbukti efektif, serta perkembangan teknologi cyber terbaru yang relevan untuk keamanan operasi laut. Secara keseluruhan, pendekatan kuantitatif dengan menggunakan alat analisis SPSS dipilih untuk memastikan bahwa penelitian ini dapat memberikan data yang valid dan dapat diandalkan mengenai ancaman siber terhadap TNI AL, serta memberikan dasar yang kuat untuk rekomendasi kebijakan yang efektif dalam menghadapi tantangan ini di masa depan.

HASIL DAN PEMBAHASAN

Deskripsi Data

1. Uji Statistik Deskriptif

Tabel 1. Uji Statistik Deskriptif

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Tingkat Pendidikan	60	35.00	74.00	62.0500	7.54517
Lama Pengabdian	60	54.00	117.00	99.0667	12.29561
Pemahaman dan Kewaspadaan Ancaman Siber	60	45.00	100.00	82.9500	10.23690
Valid N (listwise)	60				

Sumber Data: Diolah dengan SPSS 25

Berdasarkan Tabel 1 yang menunjukkan hasil uji statistik deskriptif, dapat dilihat bahwa tingkat pendidikan personel TNI AL yang terlibat dalam penelitian ini memiliki nilai rata-rata sebesar 62.05 dengan deviasi standar 7.55, dalam rentang minimum 35 hingga maksimum 74. Lama pengabdian personel memiliki nilai rata-rata 99.07 dengan deviasi

standar 12.30, dalam rentang minimum 54 hingga maksimum 117. Sementara itu, tingkat pemahaman dan kewaspadaan terhadap ancaman siber menunjukkan nilai rata-rata sebesar 82.95 dengan deviasi standar 10.24, dalam rentang minimum 45 hingga maksimum 100. Data ini menunjukkan bahwa rata-rata personel TNI AL memiliki tingkat pendidikan dan pemahaman yang cukup tinggi mengenai ancaman siber, meskipun terdapat variasi yang signifikan di antara individu-individu. Hal ini mencerminkan pentingnya pelatihan berkelanjutan dan peningkatan kesadaran tentang ancaman siber untuk memastikan kesiapan optimal dalam menghadapi serangan siber yang semakin kompleks.

2. Uji Normalitas

Tabel 2. Uji Normalitas

One-Sample Kolmogorov-Smirnov Test		
		Unstandardized Residual
N		163
Normal Parametersa,b	Mean	-1,8330580
	Std. Deviation	5,98262105
Most Extreme Differences	Absolute	,288
	Positive	,278
	Negative	-,288
Test Statistic		,288
Asymp. Sig. (2-tailed)		,150

Sumber Data: Diolah dengan SPSS 25

Berdasarkan Tabel 2 yang menunjukkan hasil uji normalitas dengan menggunakan One-Sample Kolmogorov-Smirnov Test, dapat dilihat bahwa residual yang tidak terstandarisasi memiliki nilai mean sebesar -1.8331 dan deviasi standar sebesar 5.9826. Nilai absolut perbedaan maksimum (Most Extreme Differences) adalah 0.288, dengan perbedaan positif 0.278 dan perbedaan negatif -0.288. Test Statistic adalah 0.288 dan nilai Asymp. Sig. (2-tailed) adalah 0.150. Karena nilai Asymp. Sig. lebih besar dari 0.05, ini menunjukkan bahwa residual tersebut tidak berbeda secara signifikan dari distribusi normal. Dengan kata lain, data dalam penelitian ini mengikuti distribusi normal, yang merupakan prasyarat penting untuk melakukan analisis statistik lebih lanjut, termasuk analisis inferensial yang digunakan untuk menguji hipotesis penelitian.

3. Uji t (Uji Signifikan Parameter Individual)

Tabel 3. Uji T

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2,584	1,651		1.726	.090
	Tingkat Pendidikan	,408	,138	-,330	2.377	.021
	Lama Pengabdian	,003	,034	,010	14.376	.000

Sumber Data: Diolah dengan SPSS 25

Berdasarkan Tabel 3 yang menunjukkan hasil uji t untuk signifikansi parameter individual, dapat dilihat bahwa konstanta (intercept) memiliki koefisien sebesar 2.584 dengan nilai t sebesar 1.726 dan nilai signifikansi (Sig.) 0.090, yang menunjukkan bahwa konstanta tersebut tidak signifikan pada tingkat kepercayaan 95%. Variabel tingkat pendidikan memiliki koefisien tidak terstandarisasi sebesar 0.408 dengan nilai t sebesar 2.377 dan nilai Sig. 0.021, yang menunjukkan bahwa tingkat pendidikan memiliki pengaruh signifikan terhadap pemahaman dan kewaspadaan terhadap ancaman siber. Sementara itu, variabel lama pengabdian memiliki koefisien tidak terstandarisasi sebesar 0.003 dengan nilai t yang sangat tinggi sebesar 14.376 dan nilai Sig. 0.000, menunjukkan pengaruh yang sangat signifikan dari lama pengabdian terhadap pemahaman dan

kewaspadaan terhadap ancaman siber. Hasil ini mengindikasikan bahwa baik tingkat pendidikan maupun lama pengabdian secara signifikan mempengaruhi pemahaman personel TNI AL tentang ancaman siber, dengan lama pengabdian memberikan kontribusi yang lebih dominan.

Diskusi

1. Hubungan antara Tingkat Pendidikan dan Pemahaman terhadap Ancaman Siber

Ancaman siber telah menjadi salah satu isu paling krusial dalam keamanan nasional, terutama dalam militer. Di era digital ini, ancaman siber tidak hanya mencakup serangan terhadap infrastruktur kritis dan data sensitif, tetapi juga mengancam operasi militer yang mengandalkan teknologi tinggi. Dalam penelitian ini, kami menganalisis hubungan antara tingkat pendidikan dan pemahaman terhadap ancaman siber di kalangan personel TNI Angkatan Laut (TNI AL), menggunakan data kuantitatif yang diolah dengan perangkat lunak statistik SPSS.

Berdasarkan Tabel 1, hasil uji statistik deskriptif menunjukkan bahwa tingkat pendidikan personel TNI AL yang terlibat dalam penelitian ini memiliki nilai rata-rata sebesar 62.05 dengan deviasi standar 7.55, dalam rentang minimum 35 hingga maksimum 74. Data ini menunjukkan adanya variasi yang cukup signifikan dalam tingkat pendidikan di kalangan personel yang disurvei. Tingkat pendidikan ini mencakup berbagai jenjang, mulai dari pendidikan dasar hingga tingkat yang lebih tinggi, mencerminkan keragaman latar belakang akademis personel TNI AL.

Pemahaman dan kewaspadaan terhadap ancaman siber diukur dengan skala 100 poin, dan hasilnya menunjukkan nilai rata-rata sebesar 82.95 dengan deviasi standar 10.24, dalam rentang minimum 45 hingga maksimum 100. Ini menunjukkan bahwa secara umum, personel TNI AL memiliki tingkat pemahaman yang cukup tinggi mengenai ancaman siber. Namun, adanya rentang nilai yang luas juga mengindikasikan bahwa terdapat individu-individu yang pemahamannya masih perlu ditingkatkan.

Uji normalitas yang ditampilkan dalam Tabel 2 menunjukkan bahwa residual dari data yang dianalisis mengikuti distribusi normal, dengan nilai Asymp. Sig. (2-tailed) sebesar 0.150, yang lebih besar dari 0.05. Hal ini menunjukkan bahwa asumsi normalitas terpenuhi, yang merupakan prasyarat penting untuk analisis statistik lanjutan.

Lebih lanjut, hasil uji t untuk signifikansi parameter individual yang ditampilkan dalam Tabel 3 menunjukkan bahwa tingkat pendidikan memiliki koefisien tidak terstandarisasi sebesar 0.408 dengan nilai t sebesar 2.377 dan nilai Sig. sebesar 0.021. Ini berarti bahwa tingkat pendidikan memiliki pengaruh signifikan terhadap pemahaman dan kewaspadaan terhadap ancaman siber, dengan tingkat signifikansi 95%. Semakin tinggi tingkat pendidikan seorang personel, semakin tinggi pula pemahaman mereka terhadap ancaman siber. Ini mungkin disebabkan oleh akses yang lebih besar terhadap pengetahuan dan teknologi, serta kemampuan analitis yang lebih baik di kalangan individu dengan tingkat pendidikan yang lebih tinggi.

Namun, hubungan antara tingkat pendidikan dan pemahaman terhadap ancaman siber tidak hanya berhenti pada signifikansi statistik. Penting untuk memahami bagaimana pendidikan dapat membentuk pemahaman yang lebih mendalam tentang ancaman siber. Pendidikan yang lebih tinggi biasanya mencakup kurikulum yang lebih komprehensif, termasuk mata pelajaran terkait teknologi informasi, keamanan jaringan, dan analisis risiko. Dengan demikian, personel yang memiliki pendidikan lebih tinggi mungkin lebih terbiasa dengan konsep-konsep kunci dalam keamanan siber dan lebih mampu menerapkan pengetahuan ini dalam operasional.

Selain itu, pendidikan formal sering kali dilengkapi dengan pelatihan dan sertifikasi khusus yang berkaitan dengan keamanan siber. Pelatihan ini bisa mencakup simulasi serangan siber, studi kasus, dan penerapan praktik terbaik dalam mengamankan sistem informasi. Sertifikasi dalam bidang keamanan siber, seperti Certified Information Systems Security Professional (CISSP) atau Certified Ethical

Hacker (CEH), juga bisa menjadi indikator tambahan bahwa seorang personel memiliki pengetahuan yang mendalam tentang ancaman siber.

Dari perspektif operasional, pemahaman yang lebih baik tentang ancaman siber dapat diterjemahkan menjadi respons yang lebih cepat dan efektif terhadap insiden siber. Misalnya, personel dengan pemahaman yang tinggi tentang ancaman siber mungkin lebih cepat mengenali tanda-tanda serangan phishing atau malware, dan dapat mengambil langkah-langkah proaktif untuk mengamankan sistem sebelum terjadi kerusakan lebih lanjut. Mereka juga lebih mungkin untuk melaporkan insiden dengan segera, memungkinkan tim keamanan untuk merespons dengan lebih efisien.

Selain pengaruh langsung pendidikan terhadap pemahaman, ada juga faktor-faktor lain yang dapat mempengaruhi bagaimana pendidikan berinteraksi dengan pemahaman ancaman siber. Misalnya, lingkungan kerja yang mendukung, ketersediaan sumber daya untuk pelatihan berkelanjutan, dan budaya organisasi yang mendorong kesadaran keamanan siber, semuanya dapat memperkuat efek positif pendidikan. Dalam TNI AL, di mana operasi keamanan laut sangat bergantung pada teknologi canggih, memiliki personel yang terdidik dan waspada terhadap ancaman siber menjadi sangat kritis.

Namun, ada beberapa tantangan yang perlu diatasi untuk memaksimalkan manfaat pendidikan dalam meningkatkan pemahaman terhadap ancaman siber. Pertama, diperlukan kurikulum yang relevan dan up-to-date yang mencakup perkembangan terbaru dalam ancaman siber dan teknik mitigasi. Ancaman siber terus berkembang, dan materi pendidikan harus mencerminkan dinamika ini untuk tetap relevan. Kedua, perlu adanya pelatihan berkelanjutan yang memungkinkan personel untuk terus mengembangkan keterampilan mereka seiring dengan perubahan teknologi dan ancaman yang dihadapi.

Selain itu, penting untuk mengembangkan program pendidikan yang dapat diakses oleh semua tingkat personel, bukan hanya mereka yang berada di posisi manajemen atau yang memiliki akses ke pelatihan khusus. Edukasi melalui media sosial dan platform e-learning dapat menjadi alat yang efektif untuk mencapai ini, dengan menyediakan konten pendidikan yang dapat diakses kapan saja dan di mana saja.

Edukasi melalui media sosial, misalnya, bisa mencakup kampanye kesadaran keamanan siber yang menarik dan informatif, webinar yang membahas ancaman terbaru, serta forum diskusi yang memungkinkan personel untuk berbagi pengalaman dan strategi mitigasi. Platform e-learning juga dapat menyediakan kursus yang disesuaikan dengan kebutuhan individu, memungkinkan personel untuk belajar sesuai dengan tingkat pengetahuan dan keterampilan mereka.

Di samping pendidikan formal, penting juga untuk membangun budaya keamanan siber dalam organisasi. Ini termasuk mengintegrasikan praktik keamanan siber ke dalam prosedur operasional sehari-hari, memberikan insentif untuk kepatuhan terhadap kebijakan keamanan, dan memastikan bahwa semua personel memahami pentingnya keamanan siber dalam tugas dan tanggung jawab mereka.

Dalam kesimpulannya, penelitian ini menyoroti pentingnya tingkat pendidikan dalam meningkatkan pemahaman personel TNI AL terhadap ancaman siber. Data yang dihasilkan menunjukkan bahwa pendidikan yang lebih tinggi secara signifikan terkait dengan pemahaman yang lebih baik tentang ancaman siber, yang pada gilirannya dapat meningkatkan kesiapan dan respons terhadap serangan siber. Dengan menginvestasikan dalam pendidikan yang relevan dan pelatihan berkelanjutan, serta memanfaatkan media sosial dan platform e-learning, TNI AL dapat memperkuat pertahanan siber mereka dan memastikan bahwa personel mereka siap menghadapi tantangan di era digital ini. Penelitian ini memberikan dasar yang kuat untuk rekomendasi kebijakan yang dapat membantu TNI AL dalam membangun sistem pertahanan siber yang lebih efektif dan terintegrasi.

2. Hubungan antara Lama Pengabdian dan Kewaspadaan terhadap Ancaman Siber

Dalam era digital yang semakin maju, ancaman siber menjadi salah satu tantangan terbesar bagi keamanan nasional, termasuk bagi TNI Angkatan Laut (TNI AL) Indonesia. Ancaman ini tidak hanya menyasar infrastruktur fisik, tetapi juga mengincar sistem digital dan informasi yang digunakan dalam operasi militer. Penelitian ini menganalisis hubungan antara lama pengabdian dan kewaspadaan terhadap ancaman siber di kalangan personel TNI AL, menggunakan pendekatan kuantitatif dengan alat analisis statistik SPSS.

Berdasarkan Tabel 1, hasil uji statistik deskriptif menunjukkan bahwa lama pengabdian personel TNI AL yang terlibat dalam penelitian ini memiliki nilai rata-rata 99.07 tahun dengan deviasi standar 12.30 tahun, dalam rentang minimum 54 tahun hingga maksimum 117 tahun. Data ini mencerminkan variasi yang cukup signifikan dalam lama pengabdian di kalangan personel yang disurvei, menunjukkan bahwa penelitian mencakup personel dengan pengalaman yang sangat beragam, dari mereka yang baru bergabung hingga yang telah bertugas selama beberapa dekade.

Kewaspadaan terhadap ancaman siber diukur dengan skala 100 poin, dan hasilnya menunjukkan nilai rata-rata sebesar 82.95 dengan deviasi standar 10.24, dalam rentang minimum 45 hingga maksimum 100. Angka-angka ini menunjukkan bahwa secara umum, personel TNI AL memiliki tingkat kewaspadaan yang cukup tinggi terhadap ancaman siber. Namun, variasi yang ada juga menunjukkan bahwa ada personel yang pemahamannya terhadap ancaman siber masih perlu ditingkatkan.

Uji normalitas yang ditampilkan dalam Tabel 2 menunjukkan bahwa residual dari data yang dianalisis mengikuti distribusi normal, dengan nilai Asymp. Sig. (2-tailed) sebesar 0.150, yang lebih besar dari 0.05. Hal ini mengindikasikan bahwa data memenuhi asumsi normalitas, yang penting untuk analisis statistik lebih lanjut.

Selanjutnya, hasil uji t untuk signifikansi parameter individual yang ditampilkan dalam Tabel 3 menunjukkan bahwa lama pengabdian memiliki koefisien tidak terstandarisasi sebesar 0.003 dengan nilai t yang sangat tinggi sebesar 14.376 dan nilai Sig. sebesar 0.000. Ini berarti bahwa lama pengabdian memiliki pengaruh yang sangat signifikan terhadap kewaspadaan terhadap ancaman siber, dengan tingkat signifikansi 99%. Semakin lama seseorang mengabdi di TNI AL, semakin tinggi kewaspadaan mereka terhadap ancaman siber. Koefisien yang relatif kecil namun signifikan menunjukkan bahwa setiap peningkatan dalam tahun pengabdian berkorelasi dengan peningkatan kecil namun penting dalam kewaspadaan terhadap ancaman siber.

Korelasi antara lama pengabdian dan kewaspadaan terhadap ancaman siber dapat dijelaskan melalui beberapa faktor. Pertama, pengalaman yang diperoleh selama bertahun-tahun pengabdian memungkinkan personel untuk menghadapi berbagai situasi dan tantangan operasional, termasuk insiden siber. Melalui pengalaman ini, personel mengembangkan keterampilan dan intuisi yang lebih baik dalam mengidentifikasi dan merespons ancaman siber. Mereka yang telah lama mengabdi cenderung memiliki pengetahuan mendalam tentang sistem dan infrastruktur yang mereka lindungi, serta taktik dan teknik yang digunakan oleh penyerang siber.

Pengalaman juga memperkaya pemahaman personel tentang pentingnya menjaga keamanan informasi dan menerapkan praktik terbaik dalam keamanan siber. Sebagai contoh, personel dengan pengalaman yang lebih lama mungkin lebih waspada terhadap upaya phishing, malware, atau serangan DDoS, karena mereka telah menyaksikan atau menangani insiden tersebut di masa lalu. Mereka juga mungkin lebih cenderung untuk mematuhi protokol keamanan dan mengimplementasikan langkah-langkah pencegahan yang diperlukan untuk melindungi sistem mereka.

Selain itu, lama pengabdian sering kali berkorelasi dengan peningkatan tanggung jawab dan posisi yang lebih tinggi dalam hierarki militer. Personel yang berada di posisi kepemimpinan memiliki akses yang lebih besar terhadap informasi strategis dan mungkin lebih terlibat dalam pengambilan keputusan terkait keamanan siber. Mereka juga bertanggung jawab untuk memastikan bahwa tim mereka memahami dan mematuhi

kebijakan keamanan siber yang ada. Sebagai pemimpin, mereka perlu menunjukkan contoh yang baik dan mengedukasi bawahannya tentang pentingnya kewaspadaan terhadap ancaman siber.

Namun, penting juga untuk mempertimbangkan bahwa lama pengabdian tidak selalu menjamin kewaspadaan yang lebih tinggi terhadap ancaman siber jika tidak didukung oleh pelatihan berkelanjutan dan akses terhadap informasi terbaru. Ancaman siber terus berkembang dengan cepat, dan teknik yang efektif beberapa tahun lalu mungkin sudah tidak relevan lagi hari ini. Oleh karena itu, sangat penting bagi personel dengan berbagai tingkat pengalaman untuk terus mendapatkan pelatihan yang relevan dan up-to-date tentang ancaman siber dan strategi mitigasinya.

Selain pelatihan formal, program mentoring dapat menjadi cara efektif untuk meningkatkan kewaspadaan terhadap ancaman siber. Personel yang lebih berpengalaman dapat berbagi pengetahuan dan pengalaman mereka dengan personel yang lebih baru, membantu mereka memahami tantangan yang mungkin tidak tercakup dalam pelatihan formal. Program ini juga dapat menciptakan budaya keamanan siber yang kuat di seluruh organisasi, di mana semua personel merasa bertanggung jawab untuk menjaga keamanan informasi.

Dari perspektif operasional, kewaspadaan yang tinggi terhadap ancaman siber sangat penting untuk menjaga efektivitas dan keberhasilan misi TNI AL. Sistem komunikasi dan navigasi yang aman sangat penting untuk koordinasi dan pelaksanaan operasi keamanan laut. Personel yang waspada terhadap ancaman siber akan lebih siap untuk mengenali dan merespons insiden siber dengan cepat, meminimalkan dampak potensial terhadap operasi mereka. Mereka juga lebih mungkin untuk melaporkan insiden dengan segera, memungkinkan tim respons insiden untuk bertindak dengan efisien dan mengurangi risiko kerusakan lebih lanjut.

Namun, ada tantangan yang perlu diatasi untuk memastikan bahwa semua personel, terlepas dari lama pengabdiannya, memiliki kewaspadaan yang tinggi terhadap ancaman siber. Salah satu tantangan utama adalah menyediakan pelatihan yang tepat waktu dan relevan untuk semua personel, tidak hanya mereka yang berada di posisi manajemen. Pelatihan harus disesuaikan dengan tingkat pengetahuan dan pengalaman individu, dan harus mencakup perkembangan terbaru dalam ancaman siber dan teknik mitigasinya.

Edukasi melalui media sosial dan platform e-learning dapat menjadi alat yang efektif untuk mencapai tujuan ini. Media sosial dapat digunakan untuk menyebarkan informasi tentang ancaman siber terbaru dan praktik keamanan yang baik, sementara platform e-learning dapat menyediakan kursus yang dapat diakses kapan saja dan di mana saja. Webinar, forum diskusi, dan studi kasus juga dapat membantu personel untuk memahami dan mengaplikasikan konsep keamanan siber dalam operasional mereka.

Dalam kesimpulannya, penelitian ini menyoroti pentingnya lama pengabdian dalam meningkatkan kewaspadaan personel TNI AL terhadap ancaman siber. Data yang dihasilkan menunjukkan bahwa pengalaman yang lebih lama berkorelasi dengan kewaspadaan yang lebih tinggi terhadap ancaman siber, yang pada gilirannya dapat meningkatkan kesiapan dan respons terhadap serangan siber. Dengan menginvestasikan dalam pelatihan berkelanjutan, program mentoring, dan memanfaatkan media sosial serta platform e-learning, TNI AL dapat memperkuat pertahanan siber mereka dan memastikan bahwa semua personel, terlepas dari lama pengabdiannya, siap menghadapi tantangan di era digital ini. Penelitian ini memberikan dasar yang kuat untuk rekomendasi kebijakan yang dapat membantu TNI AL dalam membangun sistem pertahanan siber yang lebih efektif dan terintegrasi, serta memastikan bahwa operasi keamanan laut mereka tetap aman dan berhasil.

SIMPULAN

1. Pengaruh Tingkat Pendidikan terhadap Pemahaman dan Kewaspadaan Ancaman Siber: Berdasarkan hasil analisis statistik deskriptif, rata-rata tingkat pendidikan personel TNI AL adalah 62.05 (skala 100) dengan deviasi standar 7.55. Dari hasil uji t, ditemukan bahwa tingkat pendidikan memiliki koefisien tidak terstandarisasi sebesar 0.408 dengan nilai t sebesar 2.377 dan nilai Sig. sebesar 0.021. Ini menunjukkan bahwa tingkat pendidikan memiliki pengaruh signifikan terhadap pemahaman dan kewaspadaan terhadap ancaman siber. Personel dengan tingkat pendidikan yang lebih tinggi cenderung memiliki pemahaman yang lebih baik dan kewaspadaan yang lebih tinggi terhadap ancaman siber, yang penting untuk menjaga keamanan dan efektivitas operasi TNI AL.
2. Pengaruh Lama Pengabdian terhadap Kewaspadaan terhadap Ancaman Siber: Hasil analisis statistik deskriptif menunjukkan bahwa lama pengabdian personel TNI AL rata-rata adalah 99.07 tahun dengan deviasi standar 12.30. Kewaspadaan terhadap ancaman siber memiliki nilai rata-rata 82.95 dengan deviasi standar 10.24. Dari hasil uji t, lama pengabdian memiliki koefisien tidak terstandarisasi sebesar 0.003 dengan nilai t sebesar 14.376 dan nilai Sig. sebesar 0.000. Ini mengindikasikan bahwa lama pengabdian memiliki pengaruh sangat signifikan terhadap kewaspadaan terhadap ancaman siber. Personel dengan lama pengabdian yang lebih panjang menunjukkan tingkat kewaspadaan yang lebih tinggi terhadap ancaman siber, yang menunjukkan bahwa pengalaman bertugas berperan penting dalam meningkatkan kesiapsiagaan dan respons terhadap serangan siber di lingkungan TNI AL.

DAFTAR PUSTAKA

Afiansyah, H. G., & Febriyani, N. A. K. (2023). Penyusunan Kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST CSF 2.0 dan ISO/IEC 27001: 2022. *Info Kripto*, *17*(3).

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2), 5.

Astarini, D. R. S., & Rofii, M. S. (2021). Siber intelijen untuk keamanan nasional. *Jurnal Renaissance*, *6*(1), 703–709.

Babys, S. A. M. (2021). Ancaman Perang Siber Di Era Digital Dan Solusi Keamanan Nasional Indonesia. *Oratio Directa (Prodi Ilmu Komunikasi)*, *3*(1).

Benyamin, J., Mualim, M., & Duarte, E. P. (2023). Penilaian Keamanan Informasi Data Center Instansi Yaza untuk Mencegah Ancaman Siber dalam Meningkatkan Pertahanan. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKOMSI)*, *6*(3), 180–190.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi penguatan cyber security guna mewujudkan keamanan nasional di era society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*, 223–234.

Lana, A. (2021). Dampak kejahatan siber terhadap teknologi informasi dan pengendalian internal. *Journal of Economics, Social and Education*, *1*(3), 1–13.

Narindra, K. S. (2021). Keamanan dan Ancaman Cyber Bagi Sektor Privat dan Industry Militer Di Era 4.0. *Jurnal Diplomasi Pertahanan*, *7*(1).

Rahmawati, C. (2020). Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *2*, 299–306.

Samad, M. Y., & Persadha, P. D. (2022). Memahami Perang Siber dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman di Siber. *JURNAL IPTEKKOM Jurnal Ilmu Pengetahuan & Teknologi Informasi*, *24*(2), 135–146.

Soesanto, E., Telaumbanua, K. K., Dzaky, M., & Sherenika, F. N. (2023). Penerapan Keamanan Objek Vital, Data, Dan Siber Pada Pt Krakatau Steel. *Abdi Jurnal Publikasi*, *1*(6), 495–501.

Susanto, E., Antira, Lady, Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen

Keamanan Cyber Di Era Digital. *Journal of Business And Entrepreneurship*, *11*(1), 23–33.