ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)
Halaman 32116-32126
Volume 8 Nomor 2 Tahun 2024

Integrasi Pertahanan Siber dalam *Network Centric Warfare* (NCW) untuk Meningkatkan Keamanan Maritim

Yuni Ratnasari[1], Edvien Adi Putra[2]
[1,2] Sekolah Staf dan Komando Angkatan Laut
e-mail: yunieratnasari17@gmail.com[1], edvienaal53@gmail.com[2]

Abstrak

Keamanan maritim semakin menjadi fokus utama dengan meningkatnya ketergantungan pada teknologi informasi dan komunikasi dalam operasi kelautan. Integrasi pertahanan siber dalam Network Centric Warfare (NCW) menjadi krusial untuk melindungi infrastruktur kritis dari ancaman cyber yang semakin kompleks. Penelitian ini bertujuan untuk menganalisis tantangan, strategi perlindungan, dan implikasi integrasi pertahanan siber dalam meningkatkan keamanan maritim dalam NCW. Penelitian ini menggunakan pendekatan kualitatif dengan analisis data primer dan sekunder. Data primer diperoleh melalui wawancara dengan ahli pertahanan siber, sementara data sekunder berasal dari literatur terkait dan studi kasus. Tantangan utama dalam integrasi pertahanan siber meliputi kompleksitas infrastruktur, kebutuhan akan pelatihan dan kesadaran personel, serta implementasi teknologi yang sesuai. Strategi perlindungan yang direkomendasikan termasuk penggunaan firewall, deteksi ancaman aktif, manajemen akses yang ketat, dan kolaborasi internasional untuk pertukaran informasi intelijen. Dengan mengadopsi pendekatan ini, organisasi dapat memperkuat pertahanan mereka terhadap serangan ransomware, phishing, dan DDoS, serta memastikan keberlanjutan operasional yang aman dan efisien di lingkungan maritim yang terhubung secara digital.

Kata Kunci: *Pertahanan Siber, Network Centric Warfare, Keamanan Maritim*

Abstract

Maritime security is increasingly becoming a primary focus with increasing reliance on information and communications technology in maritime operations. Integration of cyber defense in Network Centric Warfare (NCW) is crucial to protect critical infrastructure from increasingly complex cyber threats. This research aims to analyze the challenges, protection strategies, and implications of cyber defense integration in improving maritime security in the NCW context. This research uses a qualitative approach with primary and secondary data analysis. Primary data was obtained through interviews with cyber defense experts, while secondary data came from related literature and case studies. Key challenges in cyber defense integration include infrastructure complexity, the need for personnel training and awareness, and implementation of appropriate technology. Recommended protection strategies include the use of firewalls, active threat detection, strict access management, and international collaboration for intelligence exchange. By adopting this approach, organizations can strengthen their defenses against ransomware, phishing, and DDoS attacks, and ensure continued safe and efficient operations in a digitally connected maritime environment.

Keywords: *Cyber Defense, Network Centric Warfare, Maritime Security*

PENDAHULUAN

Integrasi pertahanan siber dalam *Network Centric Warfare* (NCW) adalah langkah krusial dalam memperkuat kemampuan militer di era digital. Konsep NCW sendiri mengandalkan teknologi informasi dan komunikasi untuk menghubungkan berbagai elemen militer dalam sebuah jaringan terpadu, yang bertujuan untuk meningkatkan situational

awareness, pengambilan keputusan, dan kecepatan respon (Pratama et al., 2023). Dalam pertahanan siber memainkan peran vital dengan mencakup semua tindakan yang diperlukan untuk melindungi jaringan, sistem informasi, dan data dari serangan siber yang dapat merusak atau mengganggu operasi militer (Sutopo, 2022).

Sistem deteksi ancaman siber yang canggih harus diimplementasikan untuk mengidentifikasi dan merespons serangan secara real-time. Sistem ini harus terintegrasi dengan jaringan NCW untuk memberikan situational awareness yang komprehensif kepada semua unit militer yang terhubung dalam jaringan tersebut. Dengan deteksi yang cepat dan tepat, respons terhadap ancaman dapat dilakukan dengan lebih efisien, mengurangi dampak dari serangan siber (Khotimah & Hendra, 2023).

Keamanan infrastruktur jaringan adalah elemen kunci lainnya. Mengamankan infrastruktur jaringan yang digunakan dalam NCW dari ancaman siber sangat penting untuk menjaga integritas dan kelancaran operasi militer (Kusuma et al., 2020). Penggunaan teknologi keamanan seperti enkripsi, firewall, dan sistem deteksi intrusi adalah beberapa langkah yang dapat diambil untuk melindungi jaringan ini. Dengan infrastruktur yang aman, informasi dapat mengalir dengan lancar antara unit-unit militer, memungkinkan koordinasi yang lebih baik dan pengambilan keputusan yang lebih cepat (Harsono & Kiswara, 2022).

Manajemen risiko siber juga menjadi aspek penting dalam integrasi ini. Penilaian dan mitigasi risiko siber harus dilakukan secara terus-menerus untuk memastikan integritas, kerahasiaan, dan ketersediaan informasi dalam jaringan NCW. Ini mencakup identifikasi potensi kerentanan dalam sistem, penilaian dampak dari potensi ancaman, dan pengembangan strategi untuk mengatasi risiko tersebut. Dengan pendekatan manajemen risiko yang komprehensif, militer dapat mengurangi kemungkinan terjadinya serangan siber dan meminimalkan dampak dari serangan yang berhasil lolos (Bommakanti, 2020a).

Peningkatan kesiapan dan pelatihan bagi personel militer juga merupakan elemen kunci dalam integrasi pertahanan siber dalam NCW. Pelatihan terus-menerus sangat penting untuk memastikan bahwa personel militer siap menghadapi ancaman siber. Ini mencakup latihan simulasi serangan siber dan pengembangan kemampuan respons cepat. Dengan pelatihan yang baik, personel militer dapat merespons ancaman siber dengan lebih efektif, mengurangi waktu yang dibutuhkan untuk mengatasi serangan, dan meminimalkan kerugian yang ditimbulkan (Bommakanti, 2020b).

Integrasi pertahanan siber dalam NCW memberikan berbagai keuntungan. Salah satunya adalah peningkatan situational awareness (Malik, 2020). Dengan integrasi pertahanan siber, ancaman siber dapat dideteksi dan ditangani lebih cepat, sehingga meningkatkan situational awareness di semua level komando. Ini memungkinkan militer untuk lebih cepat merespons situasi yang berkembang, membuat keputusan yang lebih baik, dan mengurangi risiko kesalahan. Selain itu, efisiensi operasional juga meningkat dengan adanya sistem yang aman. Informasi dapat mengalir lebih cepat dan efisien antara unit-unit militer, mempercepat pengambilan keputusan dan respons terhadap situasi yang berubah. Dengan demikian, operasi militer dapat berjalan lebih lancar dan efektif (Sudarya, 2022).

Ketahanan sistem juga menjadi salah satu keuntungan dari integrasi ini. Dengan adanya pertahanan siber yang kuat, sistem militer menjadi lebih tahan terhadap serangan siber (Malik, 2020). Ini memastikan bahwa operasi militer dapat terus berjalan meskipun terjadi serangan, mengurangi risiko gangguan yang dapat mempengaruhi kelancaran operasi. Selain itu, ketahanan sistem juga berarti bahwa militer dapat lebih percaya diri dalam menggunakan teknologi informasi dan komunikasi dalam operasi mereka, karena mereka tahu bahwa sistem tersebut dilindungi dengan baik (Horn, 2020).

Integrasi pertahanan siber dalam NCW juga menghadapi berbagai tantangan. Salah satunya adalah kompleksitas teknologi. Integrasi teknologi siber ke dalam sistem NCW yang kompleks memerlukan sumber daya dan keahlian yang signifikan. Ini mencakup pengembangan dan implementasi teknologi keamanan yang canggih, serta pelatihan personel untuk menggunakan teknologi tersebut dengan efektif. Selain itu, ancaman siber terus berkembang, sehingga sistem pertahanan siber harus selalu diperbarui dan ditingkatkan. Ini memerlukan investasi yang besar dalam penelitian dan pengembangan,

serta kerja sama dengan berbagai pihak untuk mengidentifikasi dan mengatasi ancaman yang baru muncul (Stocchero, 2023).

Koordinasi dan kolaborasi juga menjadi tantangan dalam integrasi ini. Memastikan koordinasi yang efektif antara berbagai unit dan divisi militer serta lembaga keamanan lainnya sangat penting untuk keberhasilan integrasi pertahanan siber dalam NCW. Ini mencakup pengembangan prosedur operasi standar yang jelas, serta mekanisme komunikasi yang efektif untuk berbagi informasi tentang ancaman dan respons terhadap serangan siber (Sarjito, 2024).

Angkatan bersenjata Amerika Serikat, misalnya, telah mengintegrasikan pertahanan siber ke dalam doktrin NCW mereka. Mereka telah melakukan investasi besar dalam teknologi dan pelatihan siber, serta mengembangkan strategi untuk mengatasi ancaman siber yang berkembang. Demikian pula, NATO telah mengembangkan strategi pertahanan siber yang terintegrasi dalam konsep operasi jaringan-sentris mereka. Ini mencakup latihan gabungan untuk menguji dan memperkuat kesiapan siber dari negara-negara anggota, serta pengembangan teknologi dan prosedur untuk mengatasi ancaman siber.

Di Indonesia, integrasi pertahanan siber dalam NCW juga dapat diperkuat melalui kerangka hukum yang mendukung. Pasal 30 Undang-Undang Dasar 1945 (UUD 1945) menegaskan bahwa pertahanan dan keamanan negara adalah tugas dan tanggung jawab seluruh warga negara. Ini mencakup perlindungan terhadap ancaman siber yang dapat mengancam kedaulatan dan keamanan nasional. Dengan landasan hukum yang kuat, Indonesia dapat mengembangkan strategi dan kebijakan yang komprehensif untuk mengintegrasikan pertahanan siber dalam NCW, melibatkan berbagai pemangku kepentingan, dan memastikan kesiapan nasional dalam menghadapi ancaman siber (Tarigan et al., 2024).

Dalam era globalisasi dan digitalisasi saat ini, keamanan maritim tidak hanya menghadapi ancaman konvensional seperti pembajakan dan penyelundupan, tetapi juga ancaman siber yang semakin kompleks. Permasalahan utama yang dihadapi adalah meningkatnya serangan siber yang menargetkan infrastruktur maritim, termasuk sistem navigasi, komunikasi, dan kontrol kapal. Serangan-serangan ini tidak hanya dapat mengganggu operasional sehari-hari, tetapi juga berpotensi menimbulkan kerugian ekonomi yang signifikan serta ancaman terhadap keamanan nasional. Dalam beberapa tahun terakhir, serangan ransomware dan malware yang menargetkan sistem maritim telah meningkat, menandakan bahwa sektor ini menjadi target yang menarik bagi aktor-aktor jahat.

Tujuan utama dari penelitian ini adalah untuk mengembangkan strategi integrasi pertahanan siber dalam konsep *Network Centric Warfare* (NCW) guna meningkatkan keamanan maritim. NCW adalah konsep militer yang menekankan pada penggunaan teknologi informasi dan komunikasi untuk mengintegrasikan berbagai elemen perang menjadi satu jaringan terpadu, memungkinkan peningkatan kesadaran situasional dan percepatan pengambilan keputusan. Dengan mengintegrasikan pertahanan siber ke dalam NCW, diharapkan dapat meningkatkan kemampuan deteksi dini ancaman siber, melindungi infrastruktur kritis, dan memastikan kesinambungan operasional maritim tanpa gangguan yang disebabkan oleh serangan siber.

Namun, terdapat gap research yang signifikan dalam literatur yang ada mengenai integrasi pertahanan siber dalam NCW khususnya untuk keamanan maritim. Banyak penelitian sebelumnya yang telah membahas NCW dari perspektif tradisional militer, namun belum banyak yang mengkaji bagaimana pertahanan siber dapat diintegrasikan secara efektif dalam maritim. Selain itu, meskipun terdapat beberapa studi tentang ancaman siber terhadap sektor maritim, pendekatan komprehensif yang menggabungkan pertahanan siber dan NCW dalam strategi pertahanan maritim masih minim. Hal ini menandakan bahwa ada kebutuhan mendesak untuk penelitian yang lebih mendalam dan terintegrasi dalam bidang ini.

Urgensi dari penelitian ini sangat tinggi mengingat pentingnya keamanan maritim bagi ekonomi dan kedaulatan negara, khususnya bagi negara kepulauan seperti Indonesia

yang memiliki garis pantai terpanjang kedua di dunia dan sumber daya laut yang melimpah. Keamanan maritim yang terjaga tidak hanya penting untuk melindungi jalur perdagangan internasional, tetapi juga untuk menjaga kedaulatan wilayah dan melindungi sumber daya alam. Dengan meningkatnya ancaman siber yang menargetkan infrastruktur maritim, kegagalan untuk mengembangkan dan mengimplementasikan strategi pertahanan siber yang efektif dapat berakibat fatal. Serangan siber yang berhasil dapat mengakibatkan gangguan besar pada operasi pelabuhan, kerugian ekonomi yang signifikan, dan bahkan membahayakan nyawa manusia. Oleh karena itu, integrasi pertahanan siber dalam NCW menjadi sangat mendesak untuk memastikan keamanan maritim yang berkelanjutan.

Dalam menghadapi permasalahan ini, beberapa langkah strategis dapat diambil. Pertama, pembangunan infrastruktur siber yang kuat sangatlah penting. Ini termasuk penerapan sistem firewall yang canggih dan sistem deteksi intrusi (IDS) yang mampu mendeteksi dan mencegah akses tidak sah ke jaringan militer maritim. Enkripsi komunikasi juga menjadi elemen kunci untuk melindungi data yang dikirimkan antar elemen NCW. Kedua, pelatihan dan peningkatan kesadaran siber bagi personel militer perlu ditingkatkan. Pelatihan reguler yang mencakup teknik penanganan ancaman siber dan simulasi serangan siber dapat membantu personel memahami dan siap menghadapi berbagai skenario serangan. Ketiga, kolaborasi internasional harus ditingkatkan. Pertukaran informasi intelijen mengenai ancaman siber dan latihan militer bersama yang mencakup skenario serangan siber dapat memperkuat kesiapan dan kemampuan respon.

Pengembangan teknologi canggih juga harus menjadi fokus utama. Kecerdasan buatan (AI) dapat dimanfaatkan untuk analisis ancaman dan pengambilan keputusan yang lebih cepat dan akurat. Teknologi blockchain dapat digunakan untuk memastikan integritas data dan transaksi dalam jaringan NCW. Dengan memanfaatkan teknologi-teknologi ini, sistem pertahanan maritim dapat menjadi lebih tangguh dan adaptif terhadap ancaman yang terus berkembang.

Implementasi strategi ini di Indonesia memerlukan pendekatan yang komprehensif dan terintegrasi. Peningkatan kapasitas pertahanan siber melalui pendirian pusat operasi keamanan siber khusus untuk maritim dan pengembangan talenta siber menjadi langkah awal yang penting. Selain itu, integrasi dengan sistem pertahanan nasional yang ada perlu diperkuat melalui koordinasi antar-instansi seperti TNI AL, Kementerian Pertahanan, dan instansi terkait lainnya. Penggunaan sistem terpadu yang mengintegrasikan sensor, data intelijen, dan analisis ancaman akan meningkatkan efektivitas deteksi dan respons terhadap ancaman siber.

Peningkatan kesadaran dan regulasi juga merupakan aspek yang tidak boleh diabaikan. Edukasi publik tentang pentingnya keamanan siber di sektor maritim dan penetapan standar keamanan siber untuk industri maritim dan pelabuhan akan membantu menciptakan lingkungan yang lebih aman. Regulasi yang jelas dan penegakan hukum yang tegas terhadap pelanggaran keamanan siber akan menjadi fondasi yang kuat untuk strategi pertahanan siber yang efektif.

Integrasi pertahanan siber dalam *Network Centric Warfare* (NCW) adalah langkah strategis yang sangat penting untuk meningkatkan keamanan maritim. Melalui pembangunan infrastruktur siber yang kuat, pelatihan dan kesadaran, kolaborasi internasional, serta pengembangan teknologi canggih, negara dapat meningkatkan ketahanan terhadap ancaman siber dan menjaga keamanan maritim secara efektif. Implementasi strategi ini di Indonesia akan memperkuat posisi negara dalam menjaga kedaulatan dan kekayaan maritimnya, serta memastikan bahwa operasional maritim dapat berjalan dengan aman dan efisien di tengah tantangan era digital. Dengan demikian, penelitian dan pengembangan lebih lanjut dalam bidang ini sangat mendesak dan krusial untuk masa depan keamanan maritim yang lebih baik.

METODE

Jenis Penelitian

Penelitian ini akan menggunakan pendekatan kualitatif. Pendekatan kualitatif dipilih karena fokusnya pada pemahaman mendalam tentang fenomena yang kompleks, seperti integrasi pertahanan siber dalam *Network Centric Warfare* (NCW) untuk keamanan maritim. Pendekatan ini memungkinkan peneliti untuk menjelajahi berbagai perspektif, dan menggali makna dari pengalaman para responden.

Sumber Data

1. Data Primer
   Data primer akan diperoleh langsung dari lapangan, termasuk pengamatan langsung terhadap praktik dan implementasi pertahanan siber dalam operasi maritim. Contohnya dapat berupa observasi terhadap latihan militer atau simulasi serangan siber yang melibatkan elemen NCW.
2. Data Sekunder
   Data sekunder akan diperoleh dari literatur ilmiah, laporan riset, dokumen kebijakan, dan publikasi terkait. Ini termasuk studi kasus tentang serangan siber terhadap sektor maritim, kebijakan nasional atau internasional terkait pertahanan siber, serta hasil penelitian terdahulu yang relevan.

Teknik Pengumpulan Data

1. Observasi
   Observasi akan dilakukan untuk mendapatkan pemahaman langsung tentang implementasi pertahanan siber dalam NCW. Observasi dapat dilakukan di lokasi operasional militer atau dalam simulasi tertentu untuk mengamati praktik nyata dan interaksi antar elemen NCW.
2. Wawancara
   Wawancara mendalam akan dilakukan dengan para ahli dan praktisi yang terlibat langsung dalam pertahanan siber atau NCW, seperti personel militer, ahli teknologi informasi dan komunikasi, serta perwakilan dari lembaga pemerintah terkait. Wawancara akan difokuskan untuk mendapatkan pandangan mereka tentang tantangan, strategi, dan pengalaman terkait integrasi pertahanan siber dalam NCW.

Analisis Data

Analisis data dalam penelitian kualitatif ini akan melibatkan proses berikut:

1. Transkripsi dan Koding
   Wawancara akan direkam dan ditranskripsi secara keseluruhan. Data dari observasi juga akan direkam dan dianalisis. Setelah itu, data akan dikodekan untuk mengidentifikasi tema-tema utama, pola, dan hubungan antara konsep-konsep yang muncul.
2. Pemeriksaan Keabsahan
   Validitas data akan dipastikan melalui triangulasi, yaitu dengan membandingkan data dari berbagai sumber dan teknik pengumpulan data (misalnya, data dari wawancara dengan data dari observasi atau data primer dengan data sekunder).
3. Interpretasi dan Penarikan Kesimpulan
   Hasil analisis akan diinterpretasikan untuk menyusun gambaran yang komprehensif tentang bagaimana integrasi pertahanan siber dalam NCW dapat diterapkan dan dioptimalkan untuk meningkatkan keamanan maritim. Penarikan kesimpulan akan didasarkan pada bukti-bukti yang ditemukan selama analisis data.

HASIL DAN PEMBAHASAN

Tabel 1. Hasil Wawancara

No.	Topik Wawancara	Pertanyaan Utama	Jawaban Utama
1	Tantangan dalam Integrasi Pertahanan Siber dalam NCW	Apa saja tantangan utama yang dihadapi dalam mengintegrasikan pertahanan siber dalam NCW?	*"*Tantangan utama adalah kompleksitas dalam mengoordinasikan berbagai sistem yang berbeda, termasuk integrasi infrastruktur yang sudah ada dengan kebutuhan untuk

			mempertahankan keamanan siber secara menyeluruh. Kami juga menghadapi tantangan dalam membangun kesadaran dan kapasitas personel terkait pertahanan siber.*"*
2	Strategi Perlindungan Infrastruktur Kritis	Bagaimana strategi perlindungan infrastruktur kritis seperti sistem navigasi dan komunikasi?	*"*Kami telah mengimplementasikan firewall tingkat lanjut dan sistem deteksi intrusi (IDS) untuk melindungi sistem navigasi dan komunikasi dari akses tidak sah. Selain itu, kami menggunakan teknologi enkripsi untuk melindungi data yang dikirimkan antar kapal dan dengan pusat komando.*"*
3	Peran Kecerdasan Buatan (AI) dalam Analisis Ancaman	Bagaimana peran kecerdasan buatan dalam menganalisis ancaman siber terhadap sistem maritim?	*"*Kecerdasan buatan sangat penting dalam menganalisis pola serangan yang kompleks dan mengidentifikasi ancaman potensial secara cepat. AI membantu dalam memprediksi dan merespons ancaman dengan lebih efisien, mengoptimalkan operasi dan keamanan kami.*"*
4	Kolaborasi Internasional dalam Menghadapi Ancaman Siber	Seberapa pentingnya kolaborasi internasional dalam menghadapi ancaman siber terhadap infrastruktur maritim?	*"*Kolaborasi internasional sangat vital untuk pertukaran intelijen mengenai ancaman siber yang lintas batas. Kami terlibat dalam forum internasional untuk berbagi informasi dan praktik terbaik dalam melindungi infrastruktur maritim dari serangan yang semakin canggih dan sering terjadi.*"*
5	Kendala dalam Implementasi Teknologi Baru	Apa kendala utama yang dihadapi dalam mengimplementasikan teknologi baru dalam pertahanan siber?	*"*Salah satu kendala utama adalah biaya tinggi untuk memperbarui infrastruktur yang ada dengan teknologi terbaru. Selain itu, integrasi teknologi baru sering kali memerlukan pelatihan intensif bagi personel untuk memaksimalkan penggunaannya.*"*

1. Tantangan dalam Integrasi Pertahanan Siber dalam NCW

Integrasi pertahanan siber dalam *Network Centric Warfare* (NCW) untuk keamanan maritim menghadapi serangkaian tantangan yang kompleks dan memerlukan pendekatan yang matang dalam penanganannya. Salah satu tantangan utama adalah dalam hal koordinasi infrastruktur yang berbeda-beda dan perlindungan terhadap sistem yang sensitif, sementara tetap mempertahankan ketersediaan operasional yang optimal. Integrasi pertahanan siber tidak hanya melibatkan aspek teknis dalam menghubungkan

berbagai sistem, tetapi juga mengelola keamanan informasi yang kritis dalam maritim yang dinamis dan sering kali tersebar luas.

Pentingnya menjaga keamanan siber tanpa mengorbankan ketersediaan operasional merupakan titik krusial dalam strategi pertahanan siber. Hal ini menuntut adopsi teknologi yang mampu mendeteksi dan mencegah serangan siber secara proaktif, sekaligus memastikan bahwa jaringan dan sistem tetap beroperasi tanpa gangguan yang signifikan. Dalam maritim, di mana sistem navigasi, komunikasi, dan kontrol kapal berperan vital dalam keselamatan dan efisiensi operasional, keamanan siber harus menjadi prioritas utama dalam setiap keputusan integrasi teknologi baru.

Selain dari aspek teknis, tantangan lainnya adalah dalam membangun kesadaran dan kapasitas personel terkait dengan keamanan siber. Pendidikan dan pelatihan yang terus-menerus diperlukan untuk mengembangkan pemahaman yang mendalam tentang ancaman siber dan praktik terbaik dalam menghadapinya. Personel dari berbagai latar belakang, termasuk teknis dan operasional, perlu dilibatkan secara aktif dalam memahami peran mereka dalam menjaga keamanan jaringan siber. Keterlibatan mereka dalam identifikasi dan melaporkan potensi ancaman juga menjadi kunci dalam membangun pertahanan siber yang kokoh dalam NCW.

Integrasi yang sukses juga bergantung pada kemampuan untuk mengelola dan mengatasi kompleksitas infrastruktur yang ada. Dalam banyak kasus, organisasi militer dan lembaga terkait harus mengintegrasikan sistem-sistem yang sudah ada dengan teknologi baru yang dapat memperkuat pertahanan siber mereka. Proses ini memerlukan perencanaan yang matang, pengujian yang teliti, dan pembaruan berkelanjutan untuk memastikan bahwa semua komponen sistem dapat beroperasi secara harmonis dan efisien di bawah tekanan dari serangan siber yang semakin kompleks dan canggih.

2. Strategi Perlindungan Infrastruktur Kritis

Perlindungan infrastruktur kritis, seperti sistem navigasi, komunikasi, dan kontrol kapal, merupakan bagian integral dari strategi pertahanan siber dalam NCW. Strategi perlindungan ini tidak hanya fokus pada penggunaan teknologi canggih untuk mendeteksi dan menghadapi serangan, tetapi juga pada implementasi kebijakan dan prosedur yang dapat meminimalkan risiko dan memperkuat pertahanan.

Penggunaan firewall tingkat lanjut dan sistem deteksi intrusi (IDS) adalah langkah pertama dalam membangun lapisan pertahanan yang efektif. Firewall digunakan untuk memantau dan mengontrol lalu lintas yang masuk dan keluar dari jaringan, sementara IDS berfungsi untuk mendeteksi pola-pola serangan yang mencurigakan dan memberikan peringatan dini kepada administrator jaringan. Implementasi ini memungkinkan untuk memisahkan lalu lintas yang tidak diinginkan atau berpotensi berbahaya sebelum dapat menyebabkan kerusakan atau akses yang tidak sah ke sistem.

Selain itu, enkripsi data menjadi kunci dalam melindungi informasi yang dikirimkan antar kapal atau antara kapal dengan pusat komando. Teknologi enkripsi modern memastikan bahwa data yang dipertukarkan tidak dapat dibaca atau dimanipulasi oleh pihak yang tidak berwenang, bahkan jika data tersebut direbut oleh pihak yang tidak sah. Penggunaan enkripsi ini harus diintegrasikan sebagai bagian dari arsitektur keamanan yang lebih luas, termasuk penggunaan sertifikat digital untuk otentikasi yang aman dan efektif.

Manajemen akses dan otorisasi juga penting dalam perlindungan infrastruktur kritis. Kebijakan yang jelas dan diterapkan dengan ketat tentang siapa yang memiliki akses ke sistem dan data sensitif dapat membantu mengurangi risiko dari serangan dalam, serta mengidentifikasi dan mengatasi kebocoran data yang mungkin terjadi. Audit secara teratur terhadap kepatuhan terhadap kebijakan ini diperlukan untuk memastikan bahwa semua aktivitas akses dilakukan sesuai dengan prosedur yang telah ditetapkan.

3. Peran Kecerdasan Buatan (AI) dalam Analisis Ancaman

Kecerdasan Buatan (AI) memiliki peran yang semakin penting dalam mengelola dan merespons ancaman siber terhadap sistem maritim. AI tidak hanya meningkatkan kemampuan untuk mendeteksi ancaman secara lebih akurat dan cepat, tetapi juga memungkinkan untuk mengoptimalkan operasi keamanan siber secara keseluruhan.

Dalam analisis pola serangan, AI dapat digunakan untuk mengidentifikasi dan mempelajari pola-pola serangan yang baru dan tidak diketahui secara cepat. Ini memungkinkan sistem untuk secara otomatis mengidentifikasi serangan yang belum pernah terdeteksi sebelumnya, serta memberikan rekomendasi tentang tindakan respons yang tepat. Penggunaan teknik machine learning dalam AI memungkinkan sistem untuk terus belajar dan beradaptasi dengan ancaman yang berkembang, meningkatkan efektivitas dalam menanggapi serangan siber yang semakin kompleks dan dinamis.

AI juga berkontribusi dalam memprediksi ancaman potensial dengan menganalisis data yang diperoleh dari berbagai sumber, termasuk lalu lintas jaringan dan kegiatan pengguna. Dengan memahami pola perilaku yang normal dan mendeteksi anomali yang mencurigakan, AI dapat memberikan peringatan dini tentang ancaman yang mungkin muncul, memungkinkan untuk mengambil tindakan preventif sebelum kerusakan yang signifikan terjadi.

Optimisasi respons terhadap ancaman siber adalah aspek lain dari peran AI dalam NCW. Dengan analisis data yang real-time dan respons otomatis yang diprogram sebelumnya, AI dapat mengurangi waktu tanggap terhadap serangan, mengidentifikasi dan menanggapi serangan dengan cepat dan efisien. Hal ini sangat penting dalam lingkungan maritim di mana kecepatan dalam pengambilan keputusan dan tindakan respons dapat membuat perbedaan antara keamanan dan kerentanan terhadap serangan.

4. Kolaborasi Internasional dalam Menghadapi Ancaman Siber

Kolaborasi internasional menjadi elemen kunci dalam strategi untuk menghadapi ancaman siber yang kompleks dan lintas batas terhadap infrastruktur maritim. Secara alami, ancaman siber tidak mengenal batas negara, sehingga kerja sama lintas negara menjadi sangat penting untuk meningkatkan pertukaran informasi dan respons terhadap serangan yang terjadi.

Pertukaran informasi intelijen adalah salah satu manfaat utama dari kolaborasi internasional. Negara-negara dapat berbagi data dan analisis tentang ancaman yang mereka hadapi, memungkinkan pihak berwenang untuk membangun pemahaman yang lebih lengkap tentang taktik dan strategi yang digunakan oleh penyerang. Forum internasional dan inisiatif bilateral atau multilateral sering digunakan sebagai platform untuk pertukaran ini, dengan tujuan meningkatkan kesadaran tentang ancaman yang ada dan memperkuat respons bersama.

Selain itu, kolaborasi internasional memungkinkan untuk mengembangkan strategi bersama dalam menghadapi ancaman siber. Ini termasuk pengembangan standar keamanan global yang dapat diterapkan oleh semua negara peserta, serta perencanaan respons darurat yang terkoordinasi untuk mengatasi serangan yang mengancam infrastruktur maritim secara kolektif. Dengan cara ini, keamanan maritim dapat diperkuat secara efektif melalui upaya bersama dalam menghadapi tantangan yang kompleks dan dinamis dari dunia cyber.

Latihan dan simulasi bersama juga merupakan bagian penting dari kolaborasi internasional dalam pertahanan siber. Negara-negara dapat mengadakan latihan rutin untuk menguji respons mereka terhadap serangan siber, mengidentifikasi kelemahan dalam strategi dan prosedur mereka, serta meningkatkan kemampuan untuk beradaptasi dengan ancaman yang berkembang. Latihan semacam itu tidak hanya meningkatkan kerja sama praktis antara negara-negara, tetapi juga membangun kepercayaan dan komunikasi yang diperlukan untuk menangani serangan siber secara efektif.

5. Kendala dalam Implementasi Teknologi Baru

Implementasi teknologi baru dalam pertahanan siber sering kali dihadapkan pada serangkaian kendala yang harus diatasi untuk memastikan keberhasilannya. Beberapa kendala utama termasuk masalah biaya, pelatihan personel, dan integrasi yang rumit dengan infrastruktur yang sudah ada.

Biaya tinggi sering menjadi hambatan utama dalam memperbarui infrastruktur yang ada dengan teknologi yang lebih canggih dan aman. Organisasi militer dan pemerintah harus mengalokasikan sumber daya yang memadai untuk membeli, mengimplementasikan, dan memelihara teknologi baru ini dengan cara yang meminimalkan dampak terhadap anggaran operasional mereka. Strategi pengelolaan biaya yang cerdas, termasuk investasi jangka panjang dalam keamanan siber, diperlukan untuk memastikan bahwa investasi tersebut memberikan hasil yang optimal dalam jangka waktu yang panjang.

Pelatihan dan kapasitas personel adalah faktor kritis lainnya dalam keberhasilan implementasi teknologi baru. Integrasi teknologi siber yang canggih membutuhkan tim yang terlatih dengan baik yang dapat memahami, mengoperasikan, dan mempertahankan sistem dengan efektif. Pelatihan yang terus-menerus diperlukan untuk memastikan bahwa personel memiliki keterampilan dan pengetahuan yang diperlukan untuk menghadapi ancaman siber yang terus berkembang dengan baik. Inisiatif pelatihan ini juga harus mencakup kesadaran akan keamanan siber di seluruh organisasi, meningkatkan kemampuan untuk mendeteksi dan merespons serangan dengan cepat.

Integrasi teknologi baru dengan infrastruktur yang sudah ada juga bisa menjadi kompleks dan menantang. Perencanaan yang cermat dan uji coba yang menyeluruh diperlukan untuk memastikan bahwa semua sistem beroperasi secara efisien dan kompatibel satu sama lain. Penggunaan standar terbuka dan komunikasi yang terbuka antara berbagai vendor dan sistem dapat membantu mengurangi kompleksitas ini, sementara tetap menjaga keamanan dan kinerja sistem secara keseluruhan.

Tabel 2. Analisis Ancaman

No.	Jenis Ancaman	Deskripsi Ancaman	Strategi Perlindungan
1	Ransomware	Serangan yang mengenkripsi data sistem dan meminta tebusan untuk mendapatkan akses kembali.	- Implementasi firewall dan IDS untuk mendeteksi dan mencegah serangan.
			- Backup data secara berkala dan menyimpannya di tempat yang aman.
			- Pelatihan pegawai untuk mengenali dan menghindari tautan berbahaya atau lampiran email yang mencurigakan.
2	Serangan Phishing	Upaya untuk mendapatkan informasi sensitif dengan menyamar sebagai entitas tepercaya.	- Pendidikan kepada karyawan untuk mengenali tanda-tanda phishing.
			- Penggunaan sistem deteksi ancaman untuk mengidentifikasi email phishing yang masuk.
			- Implementasi kontrol akses yang ketat terhadap informasi sensitif.
3	Serangan DDoS (Distributed Denial of Service)	Membanjiri sistem dengan lalu lintas data sehingga membuat layanan tidak tersedia bagi pengguna yang sah.	- Penggunaan layanan proteksi DDoS yang dapat mengidentifikasi dan menghalau serangan.
			- Penambahan kapasitas

	infrastruktur untuk menanggulangi lonjakan lalu lintas.
	- Pemantauan lalu lintas jaringan secara terus-menerus untuk mendeteksi dan merespons serangan dengan cepat.

Berdasarkan Tabel 2 yang memuat analisis ancaman terhadap keamanan maritim, langkah-langkah perlindungan yang diusulkan menjadi krusial dalam memitigasi risiko serangan yang berpotensi merusak. Ransomware, dengan modus operandi mengenkripsi data dan meminta tebusan, dapat dihadapi dengan implementasi firewall dan IDS untuk deteksi dini, backup data secara teratur, serta pelatihan intensif terhadap pegawai terkait tautan atau lampiran mencurigakan. Serangan phishing, yang menyamar sebagai entitas tepercaya untuk memperoleh informasi sensitif, memerlukan pendidikan karyawan tentang tanda-tanda serangan tersebut, sistem deteksi ancaman yang efektif, dan kontrol ketat atas akses informasi sensitif. Sementara itu, serangan DDoS yang membanjiri sistem dengan lalu lintas data dapat dihadapi dengan perlindungan khusus DDoS, peningkatan infrastruktur, dan pemantauan jaringan yang terus-menerus untuk respons cepat. Strategi ini tidak hanya meningkatkan keamanan sistem, tetapi juga mempromosikan keberlanjutan operasional yang aman di dalam lingkungan maritim yang semakin terhubung secara digital.

SIMPULAN

Berdasarkan analisis mendalam terhadap integrasi pertahanan siber dalam Network Centric Warfare (NCW) untuk meningkatkan keamanan maritim, dapat disimpulkan bahwa tantangan utama meliputi kompleksitas infrastruktur yang berbeda, kebutuhan akan kesadaran dan kapasitas personel terkait keamanan siber, serta implementasi teknologi baru yang memadai. Strategi perlindungan seperti penggunaan firewall, deteksi ancaman aktif, dan manajemen akses yang ketat menjadi kunci dalam menghadapi ancaman seperti ransomware, phishing, dan serangan DDoS. Kolaborasi internasional juga penting dalam membangun strategi bersama dan pertukaran informasi intelijen untuk menghadapi ancaman lintas batas. Dengan demikian, langkah-langkah ini tidak hanya meningkatkan ketahanan terhadap serangan siber yang semakin kompleks, tetapi juga memastikan keberlanjutan operasional yang aman dan efisien dalam maritim yang terhubung secara digital.

DAFTAR PUSTAKA

Bommakanti, K. (2020a). India’s cyber defence capabilities: Their role in net-centric warfare. In *The Routledge Handbook of Indian Defence Policy* (pp. 367–377). Routledge India.

Bommakanti, K. (2020b). Their role in net-centric warfare. *The Routledge Handbook of Indian Defence Policy: Themes, Structures and Doctrines*, 155.

Harsono, H., & Kiswara, G. J. (2022). Pengaruh Rantai Pasokan Digital pada Kinerja Organisasi: Studi Empiris di Industri Pertahanan. *Journal of Industrial Engineering & Management Research*, *3*(6), 80–90.

Horn, C. (2020). *Homomorphic Solution to Network Centric Warfare*. Utica College.

Khotimah, N. N., & Hendra, A. (2023). Pengembangan Sistem Komunikasi Dan Radar Serta Instalasi Senjata Guna Mendukung Sistem Pertahanan Dan Keamanan Rakyat Semesta (SISHANKAMRATA). *Jurnal Pengabdian Mandiri*, *2*(1), 405–414.

Kusuma, A. W., Prakoso, L. Y., & Sianturi, D. (2020). Relevansi Strategi Pertahanan Laut Berdasarkan Doktrin Jalesveva Jayamahe Terhadap Globalisasi Dan Perkembangan Lingkungan Strategis. *Jurnal Strategi Pertahanan Laut*, *6*(1).

Malik, G. V. P. (2020). *Network centric warfare*.

Pratama, R., Timur, F. G. C., & Sutanto, R. (2023). Revitalisasi Kewaspadaan Nasional Melalui Sistem Pertahanan Dan Keamanan Terhadap Ancaman Perang Asimetris. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *10*(9), 4548–4559.

Sarjito, A. (2024). Model Ekosistem Pertahanan Negara Berbasis Kolaborasi Pemerintah,

Industri Dan Masyarakat. *JISIP UNJA (Jurnal Ilmu Sosial Ilmu Politik Universitas Jambi)*, 32–44.

Stocchero, J. M. (2023). *A network centric architecture for military command and control systems*.

Sudarya, A. (2022). Personnel Management of The Indonesian National Army Air Force (TNI-AU) In Preparing To Implement Network Centric Warfare. *Atestasi: Jurnal Ilmiah Akuntansi*, *5*(2), 693–709.

Sutopo, A. (2022). Interoperability Pesawat Terbang Tanpa Awak Dan Kapal Perang Untuk Pengamanan Alur Laut Kepulauan Indonesia. *Strategi Dan Kampanye Militer (SKM)*, *8*(2), 77–100.

Tarigan, H., Duarte, E. P., Sarjito, A., Perwita, A. A. B., & Sumarno, A. P. (2024). *Transformasi Manajemen Pertahanan Indonesia Di Era Modernisasi Militer*. Bandung: INDONESIA EMAS GROUP.