Analisis Keamanan Siber dalam Konteks Pertahanan Maritim Indonesia

Muhamad Saiful Alam[1], Muhammad Ali Nugroho[2], Fajar Adha[3]
[1,2,3]Sekolah Staff dan Komando TNI Angkatan Laut, Indonesia
E-mail: msaifulalam60@gmail.com

Article Info
Article History
Received: 2024-06-23
Revised: 2024-07-21
Published: 2024-08-03

Keywords:
Security;
Cyber;
Defense;
Maritime;
Indonesia.

Abstract
This journal writing examines the condition of cyber security in Indonesia's maritime defense, considering the importance of protecting critical maritime infrastructure from cyber attacks. Through a qualitative approach, this study explains how the integration of defense science principles and military strategy can strengthen cyber security. Analysis is carried out on existing cybersecurity frameworks and identification of gaps that may be exploited by threat actors, both state and non-state. The results of the journal writing show that although Indonesia has carried out several initiatives to improve cyber security in the maritime sector, it turns out there is still an urgent need for a more responsive and adaptive strategy that can overcome dynamic and ongoing cyber threats. So that writing this journal can provide ideas related to the need to increase cooperation between state institutions, apart from that there is a need to develop supporting policies, as well as the need to strengthen human resources and technology.

Artikel Info
Sejarah Artikel
Diterima: 2024-06-23
Direvisi: 2024-07-21
Dipublikasi: 2024-08-03

Kata kunci:
Keamanan;
Siber;
Pertahanan;
Maritim;
Indonesia.

Abstrak
Penulisan jurnal ini mengkaji terkait dengan kondisi keamanan siber dalam pertahanan maritim Indonesia, mengingat pentingnya proteksi terhadap infrastruktur kritis maritim dari serangan siber. Melalui pendekatan kualitatif, studi ini memaparkan bagaimana integrasi prinsip-prinsip ilmu pertahanan dan strategi militer dapat memperkuat keamanan siber. Analisis dilakukan terhadap kerangka kerja keamanan siber yang ada dan identifikasi celah yang mungkin dapat dimanfaatkan oleh pelaku ancaman, baik negara maupun non-negara. Hasil penulisan jurnal menunjukkan bahwa meskipun Indonesia telah melakukan beberapa inisiatif untuk meningkatkan keamanan siber di sektor maritim, ternyata masih terdapat kebutuhan mendesak untuk strategi yang lebih responsif dan adaptif yang dapat mengatasi ancaman siber yang dinamis dan berkelanjutan. Sehingga dari penulisan jurnal ini dapat memberikan pemikiran terkait dengan perlu adanya peningkatan kerjasama antar lembaga negara, selain itu perlu adanya pengembangan kebijakan yang mendukung, serta perlu adanya penguatan sumber daya manusia dan teknologi.

I. PENDAHULUAN

Indonesia sebagai negara kepulauan terbesar di dunia, memiliki wilayah laut yang luas dan strategis. Keamanan maritim menjadi prioritas utama dalam agenda pertahanan nasional untuk melindungi kepentingan teritorial serta menjaga jalur laut yang menjadi urat nadi perdagangan internasional. Dalam beberapa dekade terakhir, ancaman terhadap keamanan maritim tidak hanya datang dari konflik fisik atau invasi teritorial, tetapi juga meliputi serangan di ranah siber. Serangan siber menjadi tantangan baru yang harus dihadapi oleh negara – negara dengan kepentingan maritim yang sangat besar, termasuk Indonesia (Morton, 2019). Penggunaan teknologi informasi dan komunikasi dalam sistem pertahanan maritim telah meningkatkan efisiensi dan efektivitas operasional. Namun, hal ini juga membawa kerentanan baru dimana infrastruktur kritikal seperti sistem radar, komunikasi kapal dan data intelijen bisa menjadi target serangan siber. Sejumlah insiden serangan siber yang telah terjadi di beberapa negara menunjukkan betapa pentingnya mengamankan aspek siber dalam strategi pertahanan maritim (Sullivan, 2021).

Di Indonesia sendiri pengembangan kapasitas keamanan siber dalam konteks pertahanan maritim masih tergolong baru dan membutuhkan perhatian lebih dari pemerintah serta *stakeholders* terkait. Kebijakan dan regulasi yang mendukung, serta kerjasama antar lembaga, baik dalam skala nasional maupun internasional, menjadi sangat krusial untuk mengatasi kelemahan sistem yang ada (Patel & Jensen, 2020). Selain itu, pengembangan sumber daya manusia yang memiliki keahlian di bidang keamanan siber juga perlu dipercepat untuk menangkal potensi ancaman yang berkembang cepat. Mengingat pentingnya keamanan siber

dalam konteks pertahanan maritim, perlu adanya analisis yang mendalam mengenai bagaimana Indonesia mengelola risiko siber dalam pertahanan maritimnya. Analisis ini diharapkan dapat memberikan *insight* dan rekomendasi bermanfaat untuk pengambilan kebijakan di masa yang akan datang.

II. METODE PENELITIAN

Penulisan jurnal ini mengadopsi pendekatan deskriptif kualitatif karena bertujuan untuk memperoleh pemahaman mendalam mengenai pandangan, respons, atau persepsi individu. Pendekatan ini memprioritaskan analisis data berupa narasi daripada penggunaan data kuantitatif atau instrumen statistik. Menurut Sulistyo-Basuki (2010), penulisan jurnal deskriptif bertujuan untuk memberikan deskripsi yang akurat dan komprehensif mengenai berbagai fenomena, termasuk aktivitas, proses dan aspek humanis yang semuanya dijelaskan melalui kata-kata yang detail (Sulistyo-Basuki, 2010).

Selanjutnya, penulisan jurnal ini dikategorikan sebagai studi kepustakaan, yang merupakan bagian dari metodologi penulisan jurnal kualitatif yang tidak mengandalkan data kuantitatif atau alat ukur statistik. Studi kepustakaan melibatkan pengumpulan data melalui sumber-sumber yang tersedia di perpustakaan seperti buku, majalah, dokumen dan narasi sejarah, tanpa melaksanakan riset lapangan. Seperti yang diuraikan oleh Mestika Zed, penulisan jurnal kepustakaan memfokuskan diri pada analisis literatur yang ada di perpustakaan untuk mendapatkan data penulisan jurnal, yang pada akhirnya mendukung pembentukan pemahaman teoretis tanpa intervensi data lapangan (Zed, 2008). Adapun penulisan jurnal ini bertujuan untuk menggali secara mendalam bagaimana Tentara Nasional Indonesia Angkatan Laut (TNI AL) dapat mengatasi hambatan di lapangan dan dapat memanfaatkan potensi yang ada dalam konteks keamanan siber. Pendekatan ini memungkinkan pengumpulan data yang detail dan reflektif terhadap situasi keamanan siber saat ini, serta strategi yang bisa diterapkan untuk mengoptimalkan pertahanan siber di lingkungan militer Indonesia.

III. HASIL DAN PEMBAHASAN

A. Strategi Pertahanan

Ilmu pertahanan sebagai disiplin ilmu yang mempelajari tentang pengelolaan sumber daya dan kekuatan nasional diberbagai kondisi damai, konflik dan pasca konflik untuk menghadapi ancaman domestik dan internasional. Ilmu ini tidak terbatas pada ancaman militer saja, tetapi juga mencakup ancaman non militer terhadap keutuhan wilayah dan keselamatan bangsa. Penekanannya adalah pada pencapaian keamanan nasional melalui pengelolaan sumber daya manusia dan geografis, baik di dalam maupun luar negeri (Supriyanto, 2014).

Strategi militer, seperti yang didefinisikan oleh Liddle Hart dan Clausewitz, dan kemudian disempurnakan oleh Andre Beaufre, merupakan seni mengerahkan kekuatan militer sesuai dengan kebijakan politik yang ditetapkan. Strategi ini juga melibatkan penggunaan sumber daya yang tersedia untuk mencapai tujuan yang bisa bersifat ofensif atau defensif, dengan tujuan utama adalah mempertahankan atau mengubah status quo (Beaufre, 1963). Definisi strategi ini juga diperluas di luar konteks militer untuk mencakup perencanaan komprehensif dalam pengaturan korporat dan organisasi, yang menjelaskan cara-cara mencapai tujuan yang telah ditentukan (Rangkuti, 2013).

Dalam konteks "Tantangan dan Peluang Penerapan *Cyber Defense* di TNI AL", pemahaman mendalam tentang ilmu pertahanan dan strategi sangat relevan. Ilmu pertahanan memberikan kerangka kerja untuk mengidentifikasi bagaimana sumber daya nasional, termasuk kapabilitas *cyber*, dapat dikelola secara efektif untuk menghadapi ancaman siber. Strategi yang dikembangkan harus mencerminkan integrasi antara kebijakan politik dan taktik militer yang bertujuan untuk dapat memperkuat pertahanan siber di TNI AL.

Fokus penulisan jurnal ini adalah pada *cyber defense* di dalam tubuh TNI AL dalam hal adanya kebutuhan yang mendesak untuk melaksanakan strategi yang adaptif dan responsif terhadap ancaman siber yang dinamis. Analisis ini akan menjelajahi bagaimana prinsip-prinsip ilmu pertahanan dan strategi militer dapat diterapkan untuk mengatasi tantangan khususnya dalam penerapan *cyber defense*. Penulisan jurnal ini juga tidak hanya bertujuan untuk mengidentifikasi ancaman yang ada, tetapi juga untuk mengusulkan metode-metode inovatif yang dapat meningkatkan resiliensi dan kapasitas pertahanan siber TNI AL dalam mendukung tujuan keamanan nasional yang lebih luas (Supriyanto, 2014).

Dalam mengevaluasi kondisi keamanan siber yang ada di sektor pertahanan maritim Indonesia, penting untuk mengintegrasikan prinsip-prinsip ilmu pertahanan. Pemahaman ini membantu dalam mengatur sumber daya nasional termasuk teknologi dan kapabilitas siber dalam menangani spektrum ancaman yang luas. Dengan melihat siber sebagai aset strategis dalam pembelaan nasional, penekanan diberikan pada pengembangan kebijakan yang memperkuat infrastruktur siber, serta pada penerapan taktik yang melindungi data dan sistem penting dari serangan. Oleh karena itu, pertahanan siber harus dikelola sebagai bagian integral dari strategi pertahanan nasional, yang mengkombinasikan kekuatan teknis dengan strategi geografis dan manusia.

Mengingat kebutuhan untuk strategi yang responsif dan adaptif, penggunaan pendekatan militer tradisional yang digambarkan oleh Beaufre (1963) dan pengayaan melalui teori korporat menawarkan kerangka kerja untuk pengembangan taktik ofensif dan defensif dalam pertahanan siber TNI AL. Keberhasilan dalam memperkuat pertahanan maritim melalui siber akan bergantung pada seberapa efektif strategi-strategi tersebut diterapkan untuk menjaga status *quo* dan mengamankan sumber daya maritim dari ancaman siber yang semakin canggih. Oleh karena itu, penulisan jurnal lebih lanjut diperlukan untuk menyelaraskan taktik pertahanan dengan risiko siber yang berkembang, serta untuk menciptakan solusi yang berkelanjutan dan efektif yang mendukung tujuan keamanan nasional yang lebih luas.

B. Ancaman Siber

Ancaman diartikan sebagai setiap tindakan yang dianggap berbahaya bagi kedaulatan negara, keutuhan wilayah dan keselamatan bangsa, baik yang berasal dari dalam maupun luar negeri (Undang – Undang Nomor 3 Tahun 2003). Dalam analisis ancaman, tiga faktor utama yang diperhatikan adalah kemampuan (*capabilities*), intensitas (*intentions*) dan celah keamanan (*vulnerabilities*) (Wahyono, 2003). Sedangkan *Cyberspace* atau ruang siber merupakan arena di mana interaksi digital terjadi dan ini menjadi penting mengingat ancaman siber yang sering melibatkan pelaku non negara seperti peretas, organisasi non pemerintah dan teroris siber yang semuanya dapat mengancam pertahanan dan kedaulatan negara (Cunningham, 2012).

Menurut McDonnell dan Sayers, ancaman siber terbagi menjadi tiga kategori antara lain ancaman perangkat keras yang melibatkan pemasangan perangkat keras dengan fungsi disruptif, ancaman perangkat lunak yang melibatkan software yang bisa mencuri atau merusak informasi dan ancaman data atau informasi yang mencakup penyebaran informasi yang dapat mengakomodir kepentingan pihak tertentu (Rahmawati, 2017). Rahmawati (2017) juga mendefinisikan kejahatan siber sebagai aktivitas yang mengancam kerahasiaan, integritas dan ketersediaan sistem atau informasi.

Analisis keamanan siber dalam pertahanan maritim Indonesia menuntut pemahaman menyeluruh tentang ancaman yang dapat mengganggu kedaulatan dan keutuhan wilayah negara. Berdasarkan Undang-Undang Nomor 3 Tahun 2003, ancaman terdefinisi sebagai segala tindakan yang merugikan kedaulatan negara dan dalam ruang siber, serangan bisa datang tidak hanya dari pelaku negara tetapi juga dari non negara seperti peretas, organisasi non pemerintah, dan teroris siber. Dengan meningkatnya interaksi digital, pentingnya menilai kemampuan, intensi dan celah keamanan menjadi krusial untuk memahami dan mengantisipasi potensi risiko dalam sektor maritim. Menurut Cunningham (2012) arena digital menjadi medan baru yang memungkinkan berbagai bentuk ancaman siber yang mengharuskan penguatan strategis dalam keamanan informasi.

Lebih lanjut, keamanan siber dalam sektor maritim harus mengatasi ancaman yang khusus berorientasi pada infrastruktur kritis maritim, yang mencakup ancaman perangkat keras, perangkat lunak dan data. Seperti yang diidentifikasi oleh Rahmawati (2017) ancaman ini meliputi instalasi perangkat keras yang disruptif, perangkat lunak yang dirancang untuk mencuri atau merusak informasi, serta penyebaran data yang bisa menguntungkan pihak tertentu. Dalam menanggapi ancaman-ancaman ini, penting untuk mengembangkan Langkah-langkah keamanan yang melindungi informasi kritikal tanpa menghambat operasional maritim. Implementasi kebijakan yang efektif dan kerjasama antar-agensi, baik pada tingkat nasional maupun internasional, menjadi esensial untuk memperkuat kapabilitas pertahanan maritim Indonesia di era digital.

IV. SIMPULAN DAN SARAN

A. Simpulan

Evaluasi keamanan siber sektor maritim Indonesia menunjukkan bahwa integrasi sumber daya nasional ke dalam strategi pertahanan siber merupakan langkah penting untuk mengatasi ancaman yang semakin kompleks. Implementasi strategi pertahanan yang dirancang oleh Supriyanto (2014) menggarisbawahi pentingnya penggunaan aset siber sebagai bagian dari pertahanan nasional untuk melindungi infrastruktur kritis. Sebagai tambahan, adopsi pendekatan adaptif dan juga responsif sebagaimana digambarkan oleh Beaufre (1963) dalam pengembangan taktik ofensif dan defensif adalah esensial untuk menjaga keutuhan wilayah maritim. Oleh karena itu, pengembangan strategi pertahanan harus memprioritaskan perlindungan aset siber, dengan memanfaatkan teknologi terkini dan taktik operasional yang memadai.

Menyikapi ancaman siber yang tidak hanya bersifat militer namun juga melibatkan pelaku non negara, Indonesia perlu mempertajam penilaian kemampuan, intensi dan celah keamanan sesuai dengan realitas yang dihadapi. Hal ini dikarenakan serangan siber dapat datang dari berbagai arah dan memiliki berbagai bentuk, peningkatan kapasitas intelijen siber untuk mengidentifikasi dan menanggapi ancaman secara efektif menjadi krusial. Langkah ini akan melibatkan peningkatan kemampuan teknis dan sumber daya manusia dalam mengelola dan memitigasi risiko siber, serta memastikan bahwa tindakan pertahanan siber bisa berjalan sinergis dengan operasi maritim yang ada.

Dari analisis yang dilakukan, dapat disimpulkan bahwa kondisi keamanan siber dalam pertahanan maritim Indonesia masih membutuhkan peningkatan di beberapa aspek. Kerjasama antar lembaga dan peningkatan kebijakan yang mendukung merupakan faktor kunci dalam memperkuat keamanan siber. Hal ini termasuk pengembangan infrastruktur siber yang lebih tangguh dan peningkatan keahlian siber di kalangan personel pertahanan. Kerjasama internasional juga penting untuk berbagi intelijen dan praktek terbaik dalam menghadapi ancaman siber global yang berkembang.

B. Saran

Berdasarkan kesimpulan tersebut, rekomendasi utama adalah memperkuat kebijakan keamanan siber dengan memperhatikan perkembangan terkini dalam teknologi informasi dan komunikasi. Pengadaan teknologi canggih dan pelatihan berkelanjutan untuk sumber daya manusia di sektor pertahanan maritim harus menjadi prioritas. Selain itu, pemerintah harus mengintensifkan kerjasama dengan negara lain dan organisasi internasional untuk meningkatkan kapabilitas deteksi dan respons terhadap ancaman siber, serta mengembangkan strategi proaktif untuk memitigasi risiko yang mungkin timbul dari celah keamanan yang ada.

DAFTAR RUJUKAN

Beaufre, A. (1963). An Introduction to Strategy. Faber and Faber.

Cunningham, C. (2012). Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. CRC Press.

McDonnell, T., & Sayers, J. (2017). Understanding Cyber Warfare: Politics, Policy and Strategy. Routledge.

Patel, K., & Jensen, B. (2020). Cybersecurity for Critical Infrastructure: A Global Perspective. Springer.

Pearce II, J. A., & Robinson, R. B. (2008). Strategic Management: Formulation, Implementation, and Control. McGraw-Hill.

Rahmawati, D. (2017). Cyber Crime and Security in Indonesia. Pustaka Pelajar.

Rangkuti, F. (2013). Strategi Promosi yang Kreatif dan Analisis Kasus Integrated Marketing Communication. Gramedia Pustaka Utama.

Stoner, J. A., Freeman, R. E., & Gilbert, D. R. (2005). Management. Prentice Hall.

Supriyanto, M. (2014). Ilmu Pertahanan: Teori dan Praktik di Indonesia. Graha Ilmu.

Sullivan, J. (2021). Cybersecurity: Strategies for Cyber Defense. Wiley.

Undang-Undang Nomor 3 Tahun 2003 tentang Pertahanan Negara. (2003).

Wahyono, E. (2003). Menganalisa Ancaman terhadap Keamanan Nasional. Rajawali Pers.