Pentingnya Peran Intelegent TNI Angakatan Laut dalam Memperkuat Keamanan *Cyber* Guna Menjaga Integritas, Kerahasiaan dan Ketersediaan Data

Budi Titiono[1], Abdul Kadir Mulku Zahari[2], Muhammad Taufik Kurniawan[3]
[1,2,3]Sekolah Staff dan Komando TNI Angkatan Laut, Indonesia
E-mail: budtiti22@gmail.com

Article Info
Article History
Received: 2024-08-07
Revised: 2024-09-22
Published: 2024-10-05

Keywords:
Kamikaze Drone;
Security;
Cyber;
Intel TNI AL;
Integrity;
Confidentiality;
Data Availability.

Abstract
The purpose of writing this journal is to identify how important and urgent cyber security is in the military world, especially in the data security of the Indonesian Navy (TNI AL) in order to maintain the integrity, confidentiality and availability of data carried out by Intel personnel in the Navy dimension. This is because recently the National Data Center (PDN) has experienced disruption due to ransomware attacks that have worried various groups, especially the government. So with this problem, this journal will discuss the importance of strengthening the cyber security of the TNI AL in order to maintain the integrity, confidentiality and availability of data through efforts that should be made by institutions, especially the Ministry of Defense or Intel personnel in the Navy. The method used in writing this journal is a qualitative method with data collection through in-depth analysis of articles or journals and related news. The results of writing this journal are expected to provide in-depth insight into the dangers of cyber security disruptions and how to overcome them so that they do not have implications for the security of defense data and state security.

Artikel Info
Sejarah Artikel
Diterima: 2024-08-07
Direvisi: 2024-09-22
Dipublikasi: 2024-10-05

Kata kunci:
Keamanan;
Cyber;
Intel TNI AL;
Integritas;
Kerahasiaan;
Ketersediaan Data.

Abstrak
Penulisan jurnal ini bertujuan untuk mengidentifikasi seberapa penting dan urgensinya keamanan *cyber* dalam dunia militer khususnya pada keamanan data Tentara Nasional Indonesia Angkatan Laut (TNI AL) guna menjaga integritas, kerahasiaan dan ketersediaan data yang dilakukan oleh personal Intel pada matra Laut. Hal ini dikarenakan pada akhir-akhir ini Pusat Data Nasional (PDN) mengalami gangguan akibat dari serangan *ransomware* yang telah mengkhawatirkan berbagai kalangan khususnya pemerintah. Maka dengan adanya masalah tersebut jurnal ini akan membahas terkait dengan pentingnya memperkuat keamanan *cyber* TNI AL guna menjaga integritas, kerahasiaan dan ketersediaan data melalui upaya-upaya yang seharusnya dilakukan oleh Lembaga khususnya Kementerian Pertahanan atau personal Intel di Angkatan Laut. Adapun metode yang digunakan dalam penulisan jurnal ini adalah metode kualitatif dengan pengumpulan data melalui analisa mendalam dari artikel atau jurnal dan berita terkait. Hasil penulisan jurnal ini diharapkan dapat memberikan wawasan yang mendalam tentang bahaya dari gangguan keamanan *cyber* dan bagaimana cara penanggulanginya agar tidak berimplikasi pada keamanan data pertahanan dan keamanan negara.

I. PENDAHULUAN

Southeast Asia Freedom of Expression Network (SAFEnet) mengkritik langkah pemerintah dalam mengatasi gangguan Pusat Data Nasional (PDN) akibat serangan *ransomware* yang terjadi pada bulan Juni 2024, serangan tersebut meng-akibatkan PDN lumpuh selama 5 hari berturut-turut. Pelayanan Direktorat Jenderal Imigrasi merupakan salah satu pelayanan publik yang sangat terdampak, akibatnya terjadi antrian berjam-jam dalam penggunaan sistem manual pelayanan paspor dan visa, selain itu gangguan ini juga berimplikasi pada risiko kebocoran data secara besar-besaran. Melalui siaran pers Nomor: 409/HM/KOMINFO/06/2024 pemerintah me-nyatakan bawah Badan *Cyber* dan Sandi Negara (BSSN), Kepolisian Republik Indonesia, Kementerian dan Lembaga terkait serta PT Telkom Indonesia terlibat dalam proses pemulihan data. Pemerintah juga menyatakan bahwa PDN banyak sekali menyimpan data pribadi dan rahasia, apabila PDN mengalami kebocoran tentunya hal ini akan menimbulkan ancaman bagi keamanan nasional secara keseluruhan.

Organisasi yang memperjuangkan hak-hak digital, termasuk hak akses internet, hak kebebasan berekspresi dan hak rasa aman di ranah digital telah memberikan pernyataan bahwa sejak awal rencana pembangunan PDN awalnya menuai kritik dan kontroversi. Membangun pusat data yang mengintegrasikan

penyimpanan justru menimbulkan risiko kebocoran data yang lebih besar. Kurangnya transparansi perencanaan dan kelemahan penanganan ancaman *cyber* dari DPR dan pelaku industri akan mengakibatkan dampak yang signifikan, hal ini bisa dilihat dari adanya kasus contoh keterlibatan dana asing dari proses pembentukan awal hingga akhir bahwa PDN dikelola oleh pemerintah sendiri bukan oleh pelaku usaha di bidang industri *cloud computing* atau pusat data nasional, maka rentan sekali pembobolan data yang dilakukan oleh para peretas untuk mendapatkan keuntungan sebanyak - banyaknya. Ditambah SAFEnet juga memberikan contoh dari deretan kasus pembobolan data di Indonesia terutama yang melibatkan kementerian dan lembaga negara, sehingga hal ini tentunya semakin menunjukkan bahwa pemerintah tidak serius dalam memperkuat keamanan *cyber*.

Berdasarkan amanat Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik pasal 27 dan 30 *jo* Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional yang memberikan aturan terkait dengan penggunaan infrastruktur Sistem Pemerintahan Berbasis Elektronik (SPBE) yang memiliki tujuan untuk meningkatkan efisiensi, keamanan dan kemudahan integrasi dalam rangka memenuhi kebutuhan Infrastruktur SPBE bagi internal Instansi Pusat dan Pemerintah Daerah. Sehingga dengan adanya regulasi tersebut seharusnya pemerintah mampu menjaga seluruh akses data yang dimiliki oleh masyarakat khususnya data pada Kementrian atau Lembaga pemerintah terkait.

Adapun kerusakan PDN saat ini menunjukkan kurangnya komitmen dan juga konsistensi pemerintah dalam pembangunan infrastruktur vital yang diklaim aman dan terpercaya, sehingga hal ini menimbulkan *Single Point of Failure* (SPOF) atau titik kegagalan. Kebocoran data warga di institusi pemerintahan masih sering terjadi. Gangguan berkepanjangan pada PDN menambah hilangnya kepercayaan publik. Menurut SAFEnet, tahun 2023 ada 32 insiden kebocoran data di lembaga pemerintah, termasuk BPJS Kesehatan, Polri, KPU dan Kementerian Pertahanan. Serangan terhadap PDN dan potensi kebocoran data pribadi warga negara hanya puncak dari lemahnya sistem keamanan *cyber* Indonesia. Sehingga dengan adanya fakta tersebut maka jurnal ini akan membahas terkait dengan pentingnya peran intelegent TNI AL dalam memperkuat keamanan *cyber* guna menjaga integritas, kerahasiaan dan ketersediaan data. Mengingat bahwa dengan adanya memperkuat keamanan *cyber* pada TNI AL diharapkan dapat melindungi integritas, kerahasiaan dan ketersediaan sistem informasi dan komunikasi pada aspek yang dimilikinya.

II. METODE PENELITIAN

Adapun metode dalam menulis artikel jurnal ini yaitu menggunakan metode kualitatif dengan pengumpulan data melalui analisa mendalam dari artikel atau jurnal dan berita terkait (Muhammad Rizal, 2021) yang dideskripsikan secara induktif (Raco, 2010) sehingga diharapkan dengan adanya metode kualitatif tersebut dapat menemukan permasalahan dan solusi pada data yang diteliti secara cepat sehingga keterhubungan dalam mempengaruhi data satu sama lain memberikan struktur analisis yang eksplisit (Muhammad Rizal, 2021).

III. HASIL DAN PEMBAHASAN

A. Tugas Pokok Intelegent TNI Angkatan Laut

Pada pasal 47 Undang – Undang Nomor 34 Tahun 2004 tentang TNI disebutkan bahwa prajurit aktif dapat menduduki jabatan pada kantor yang membidangi koordinator bidang Politik dan Keamanan Negara, Pertahanan Negara, Sekretaris Militer Presiden, Intelijen Negara, Sandi Negara, Lembaga Ketahanan Nasional, Dewan Pertahanan Nasional, Search and Rescue (SAR) Nasional, Narkotika Nasional, dan Mahkamah Agung. Sehingga dengan adanya pasal tersebut maka personal intel dalam bertugas di TNI Angkatan Laut menjadi sangat penting dalam menghadapi berbagai ancaman, baik ancaman nyata maupun tidak nyata guna menjaga pertahanan dan keamanan negara, tugas-tugas dalam menjaga keamanan dan pertahanan negara yang dilakukan oleh TNI khususnya personal yang menjabat sebagai intel sudah tertuang dalam Undang-Undang Nomor 34 Tahun 2004 Pasal 6 dan 7 yang mewajibkan seluruh personal TNI harus menjaga wilayah laut secara maksimal terutama pada wilayah-wilayah perbatasan yang tidak terjangkau oleh pemerintah. Berikut adalah beberapa tugas utama personal intel TNI pada matra Laut dalam konteks ini adalah:

1. Pengawasan dan Patroli

   TNI Angkatan Laut bertanggung jawab untuk melakukan pengawasan dan patroli di perairan Indonesia, termasuk perbatasan

laut, zona ekonomi eksklusif (ZEE) dan wilayah kepulauan. Hal ini termasuk deteksi dini terhadap aktivitas ilegal seperti *illegal fishing*, perdagangan narkoba dan kegiatan ilegal lainnya.

2. Pertahanan Kedaulatan

   TNI Angkatan Laut memiliki peran dalam menjaga kedaulatan negara di laut, termasuk melindungi perairan Indonesia dari ancaman seperti invasi asing atau upaya mengklaim wilayah yang melanggar hukum internasional.

3. Penanggulangan Ancaman Terorisme

   Menghadapi ancaman terorisme, TNI Angkatan Laut bekerja sama dengan pihak-pihak terkait untuk mencegah dan menanggulangi aktivitas teroris yang melibatkan perairan sebagai jalur atau tujuan.

4. Penanggulangan Pencurian Sumber Daya Alam

   TNI Angkatan Laut turut serta dalam mengawasi dan menanggulangi pencurian sumber daya alam di perairan Indonesia, seperti pencurian ikan secara ilegal dan eksploitasi ilegal sumber daya alam lainnya.

5. Kerja Sama Internasional

   Melalui kerja sama bilateral dan multilateral, TNI AL berperan aktif dalam menjaga stabilitas dan keamanan regional, termasuk menghadapi tantangan bersama seperti piranti laut dan ancaman keamanan lainnya.

6. Pengembangan Kapabilitas

   TNI AL terus mengembangkan kapabilitasnya dalam bidang teknologi, pelatihan personel dan peralatan militer guna meningkatkan kemampuan operasionalnya dalam menghadapi ancaman yang semakin kompleks di laut.

Untuk menjalankan tugas-tugas tersebut dengan baik, seluruh personal intel TNI AL sangat bergantung pada data dukung baik data primer dan sekunder yang dibutuhkan dalam menjalankan misi pertahanan dan keamanan negara dari pemerintah. Sehingga keamanan *cyber* dapat berperan penting dalam membantu tugas dari Angkatan Laut dalam menjaga keamanan nasional Indonesia yang sangat luas dan strategis.

B. Urgensi Pentingnya Keamanan *Cyber* Dalam Dunia Militer Khususnya Pada Keamanan Data TNI Angkatan Laut

Keamanan menurut Buzan dan Hansen merupakan upaya untuk mengamankan sesuatu baik itu negara, individu, kelompok etnik, lingkungan hidup atau bahkan keberlangsungan planet bumi itu sendiri. Sedangkan urgensi jika dilihat dari bahasa latin berasal dari kata "*urgere*" yaitu (kata kerja) yang berarti mendorong. Jika dilihat dari bahasa Inggris bernama "*urgent*" (kata sifat) dan dalam bahasa Indonesia "urgensi" (kata benda). Istilah urgensi merujuk pada sesuatu yang mendorong kita, yang memaksa kita untuk diselesaikan. Dengan demikian kata urgensi digunakan pada saat ketika ada suatu masalah dan harus segera ditindaklanjuti. Sekalipun ancaman kejahatan di dunia *cyber* sudah sangat nyata, tetapi tanggapan, reaksi dan kesadaran negara atas ancaman tersebut sangat beragam karena adanya perbedaan tingkat penguasaan dan pemanfaatan, ketergantungan pada teknologi informasi yang berbeda, perbedaan tersebut berakibat pula pada cara dan tingkat penanganan kasus-kasus yang terjadi. Sehingga menurut Kepala Pusat Informasi dan Humas Kementerian Kominfo Gatot Dewa Broto dalam Siaran Pers Nomor 83/PIH/KOMINFO/11/2013 terkait dengan ancaman *cyber tttack* dan urgensinya pada keamanan informasi Nasional mengatakan bahwa terdapat tiga pendekatan untuk mempertahankan keamanan di dunia *cyber* khususnya bagi TNI AL dalam menjaga semua data yang dimilikinya, antara lain:

1. Pendekatan sosial budaya, dalam arti memberikan pemahaman dari sudut sosial budaya agar masyarakat memahami secara benar tentang kepedulian akan keamanan informasi khususnya fenomena dalam dunia *cyber* yang bersifat global dan lintas batas (*borderless*).
2. Pendekatan tata kelola dan teknologi keamanan informasi, yang dalam hal ini pendekatan dilakukan melalui sistem manajemen keamanan informasi serta melalui pendekatan teknologi yang cermat dan akurat serta *up to date* agar dapat menutup setiap lubang atau celah yang dapat digunakan untuk melakukan penyerangan-penyerangan dalam dunia *cyber*.
3. Pendekatan hukum yaitu tersedianya instrumen hukum positif nasional yang

terkait dengan pemanfaatan teknologi informasi seperti Undang – Undang Nomor 11 Tahun 2008 tentang ITE dan Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronika (PSTE) yang salah satunya adalah kebijakan dan regulasi di bidang keamanan informasi.

Keamanan *cyber* memiliki urgensi yang sangat tinggi dalam dunia militer, khususnya untuk TNI AL guna menjaga pertahanan dan keamanan negara. Hal ini dikarenakan keamanan *cyber* dapat memberikan perlindungan sistem informasi dan komunikasi data, mengingat kerahasiaan informasi dan keamanan komunikasi data pada TNI AL berfungsi untuk mengelola data dan informasi yang sangat rahasia, termasuk rencana operasi, informasi intelijen dan data strategis lainnya. Sehingga keamanan *cyber* yang kuat dapat memastikan bahwa informasi data tidak bocor atau tidak dapat diakses oleh pihak yang tidak berwenang. Selain itu sistem komunikasi militer harus aman dari penyadapan dan gangguan terlebih lagi di wilayah perbatasan yang sangat rawan terhadap akses pihak asing dalam memasuki wilayah NKRI, disini fungsi keamanan *cyber* dapat membantu melindungi jaringan komunikasi agar tetap berfungsi dengan baik dan aman dari intersepsi musuh. Saat ini TNI AL juga menggunakan berbagai sistem senjata yang terintegrasi dengan teknologi digital, adanya serangan *cyber* dapat menonaktifkan atau mengganggu sistem kerja dari seluruh data yang dimiliki oleh TNI AL, sehingga hal ini dapat melemahkan kapabilitas tempur dan pertahanan negara. Maka dari itu usaha yang harus dilakukan oleh keamanan *cyber* adalah perlunya melindungi infrastruktur ini dari serangan yang bisa mengganggu operasional sehari-hari pada pangkalan militer, pelabuhan dan kapal-kapal perang yang kesemua itu bergantung pada sistem digital.

Berbagai negara maupun kelompok non negara dapat melancarkan serangan *cyber* sebagai bagian dari strategi perang asimetris. Keamanan *cyber* yang efektif dapat membantu TNI AL dapat mendeteksi dan menanggapi serangan-serangan tersebut dengan cepat. Sehingga hal ini kemampuan untuk melaksanakan operasi *cyber* secara defensif maupun ofensif menjadi semakin penting dalam konflik modern, mengingat bahwa TNI AL membutuhkan infrastruktur dan keahlian yang kuat untuk melaksanakan operasi tersebut dikarenakan serangan *cyber* yang sukses dapat mengganggu operasi militer dan misi-misi penting. Dengan memastikan keamanan *cyber*, TNI AL dapat menjaga kontinuitas operasional dan memastikan misi-misi dapat dilaksanakan tanpa ada hambatan, hal ini tentunya untuk menjaga integritas, kerahasiaan dan ketersediaan data. Maka apabila TNI AL mengalami gangguan keamanan dipastikan TNI AL dapat merespon dengan cepat dan efektif terhadap permasalahan pada keamanan *cyber*, hal ini penting untuk meminimalkan dampak dari serangan *cyber* terhadap pertahanan dan keamanan negara.

C. Upaya Personil Intel TNI Angkatan Laut Guna Menjaga Integritas, Kerahasiaan dan Ketersediaan Data dengan Mengamankan Data *Cyber*

Secara etimologis, integritas berasal dari bahasa latin *integer* yang berarti keseluruhan atau lengkap (Fachrudin, 2013). Menurut Kamus Besar Bahasa Indonesia, integritas adalah kualitas, sifat atau keadaan yang menunjukkan suatu kesatuan yang utuh sehingga memiliki potensi dan kemampuan untuk memancarkan wibawa dan kejujuran. Semakin baik integritas sebuah Lembaga maka semakin baik pula kinerja yang dihasilkan, integritas merupakan bentuk tanggung jawab seseorang maupun kelompok Lembaga atas apa yang dilakukannya dan hasilnya sesuai dengan norma, nilai atau prinsip yang benar dan pendirian yang teguh tanpa paksaan dari pihak manapun. Adapun yang dimaksud dengan kerahasiaan adalah praktik pertukaran informasi antara sekelompok orang maupun Lembaga yang dapat menyembunyikan hasil kinerjanya terhadap orang atau Lembaga lain yang bukan anggota kelompok tersebut. Sehingga adanya urgensi terhadap keamanan *cyber* terhadap Lembaga TNI khususnya TNI AL dapat menjaga integritas, kerahasiaan maupun tersediaan data agar bisa mencegah dari tindak pidana peretasan.

Keamanan data *cyber* sangat penting di Indonesia khususnya bagi TNI AL, hal ini dikarenakan infrastruktur kritis alutsista dan alpahankam TNI bergantung pada sistem digital. Serangan *cyber* pada infrastruktur ini dapat mengakibatkan kekacauan dan ancaman

serius terhadap keamanan dan pertahanan nasional. Di Indonesia, peningkatan insiden keamanan *cyber* seperti peretasan dan pencurian data menunjukkan pentingnya memperkuat langkah-langkah keamanan *cyber*. Sehingga untuk memperkuat keamanan *cyber* guna menjaga integritas, kerahasiaan dan ketersediaan data yang dilakukan oleh personil intel TNI AL, antara lain :

1. Personal intel TNI AL telah mengambil Langkah-langkah untuk meningkatkan keamanan *cyber* melalui regulasi dan inisiatif dengan cara berkoordinasi dengan pemerintah yang memegang wewenang itu (Lembaga legislatif)
2. Untuk melaksanakan keamanan *cyber*, personal intel TNI AL tidak bisa berjalan dengan sendirinya, maka memerlukan mitra dalam menangkal hal-hal tersebut salah satunya bekerjasama dengan Kementerian atau Lembaga terkait
3. Keamanan *cyber* yang kuat memungkinkan personal intel TNI AL untuk berkoordinasi secara aman dengan sekutu dan mitra internasional, hal ini penting untuk operasi gabungan dan latihan militer yang melibatkan berbagai negara. Sehingga dalam kolaborasi internasional, kepercayaan terhadap keamanan data sangat penting, mitra internasional harus yakin bahwa informasi yang mereka bagikan dengan TNI AL akan dilindungi dengan baik.
4. Personal intel TNI AL juga melakukan pengembangan terhadap personel militer yang harus dilatih dalam praktik-praktik keamanan *cyber* untuk mengurangi risiko *human error* yang dapat dimanfaatkan oleh musuh.
5. Personal intel TNI AL melakukan pengembangan keahlian teknis dalam bidang keamanan *cyber,* hal ini sangat penting untuk mengidentifikasi dan mengatasi ancaman *cyber* yang semakin kompleks.

Sehingga dengan memperkuat keamanan *cyber*, TNI AL dapat menjaga integritas, kerahasiaan dan ketersediaan sistem-sistem kritis yang mereka gunakan serta dapat memastikan pertahanan negara Indonesia tetap kuat dan siap menghadapi berbagai ancaman modern.

IV. SIMPULAN DAN SARAN

A. Simpulan

Tugas personal intel TNI Angkatan Laut di Indonesia sangat penting dalam menghadapi berbagai ancaman, baik ancaman nyata maupun tidak nyata guna menjaga pertahanan dan keamanan negara, tugas tersebut sudah tertuang dalam Undang-Undang Nomor 34 Tahun 2004 Pasal 6 dan 7 yang mewajibkan seluruh personal TNI harus menjaga wilayah laut secara maksimal terutama pada wilayah-wilayah perbatasan yang tidak terjangkau oleh pemerintah. Untuk menjalankan tugas-tugas tersebut dengan baik, personal intel TNI AL sangat bergantung pada data dukung baik data primer dan sekunder yang dibutuhkan dalam menjalankan misi pertahanan dan keamanan negara dari pemerintah. Selain itu keamanan *cyber* dapat berperan penting dalam membantu tugas dari setiap personal intel TNI AL dalam menjaga keamanan nasional Indonesia yang sangat luas dan strategis. Mengingat keamanan *cyber* memiliki urgensi yang sangat tinggi dalam dunia militer, khususnya bagi TNI AL dalam menjaga pertahanan dan keamanan negara. Hal ini dikarenakan keamanan *cyber* dapat memberikan perlindungan sistem informasi dan komunikasi data, mengingat kerahasiaan informasi dan keamanan komunikasi data pada TNI AL berfungsi untuk mengelola data dan informasi yang sangat rahasia, termasuk rencana operasi, informasi intelijen dan data strategis lainnya guna menjaga integritas, kerahasiaan dan ketersediaan data.

B. Saran

Pembahasan terkait penelitian ini masih sangat terbatas dan membutuhkan banyak masukan, saran untuk penulis selanjutnya adalah mengkaji lebih dalam dan secara komprehensif tentang Pentingnya Peran Intelegent TNI Angakatan Laut dalam Memperkuat Keamanan *Cyber* Guna Menjaga Integritas, Kerahasiaan dan Ketersediaan Data.

DAFTAR RUJUKAN

"Secret Quotes". Diarsipkan dari versi asli tanggal 2006-05-16. Diakses tanggal 2006-12-24.

Abdurrahman Saleh dan Muhbib Abdul Wahab, Psikologi Suatu Pengantar dalam Perspektif Islam, (Jakarta: Kencana, 2004), hlm. 89.

Astia Pamungkas, Pengertian Esensi dan Urgensi, artikel, diakses tanggal 14 Juni 2016, pukul 14.15.

Aware ID Analisis Singkat Insiden Keamanan *Cyber* PDNS dan Rekomendasi Untuk Perbaikan file:///C:/Users/DWI%20NURIL/Downloads/ANALISIS%20SINGKAT%20INSIDEN%20KEAMANAN%20*CYBER*%20PDNS%20DAN%20SARAN.pdf

Barry Buzan and Lenen Hansen, The Evolution of International Security Studies, (United Kingdom: Cambridge University Press, 2009) hal. 10-13.

Berita suara.com https://www.suara.com/bisnis/2024/06/25/153815/safenet-kritik-keras-pemerintah-penanganan-serangan-*cyber*-di-pdn-amatiran

J. Sarwono, "Metode Penelitian Kuantitatif dan Kualitatif," 2006.

Nazir, "Metode Penelitian.," Ghalia Indonesia, 1988.