JURNAL MAHATVAVIRYA Vol. 12. No. 2. Sep 2025 P-ISSN: 2355-5262
DOI: https://10.63824/mahatvavirya E-ISSN: 2963-8607

PERAN STRATEGIS TEKNOLOGI INFORMASI DAN KOMUNIKASI DALAM OPERASI MILITER TNI AD

Hiras M. S. Turnip
Dislitbang TNI AD
hirasturnip@gmail.com

Abstract

This study examines the implementation of information and communication technology (ICT) in supporting military operations within the Indonesian Army (TNI AD). Using a qualitative literature review approach, the research identifies the current state, benefits, challenges, and development prospects of ICT in the TNI AD. The findings reveal that ICT implementation has improved operational effectiveness through systems such as the Battle Management System (BMS), Integrated Command and Control System (ICCS), and personnel as well as logistics data management applications. However, challenges remain, including limited long-range communication infrastructure, low integration between information systems, human resource constraints, and cybersecurity threats. A comparison with the best international practices shows significant gaps that must be addressed through infrastructure strengthening, system integration, human resource capacity building, and international collaboration. Strategic recommendations include developing a high-capacity communication backbone, creating an integrated system roadmap, providing continuous training, enhancing cyber defense, and advancing ICT-based defense diplomacy.

Keywords: *Information and Communication Technology, Indonesian Army, Military Operations, Network Centric Warfare, Cybersecurity.*

Abstrak

Penelitian ini mengkaji implementasi teknologi informasi dan komunikasi (TIK) dalam mendukung operasional militer di lingkungan Tentara Nasional Indonesia Angkatan Darat (TNI AD). Menggunakan pendekatan kualitatif berbasis studi literatur, penelitian ini mengidentifikasi kondisi aktual, manfaat, tantangan, dan prospek pengembangan TIK di TNI AD. Hasil kajian menunjukkan bahwa penerapan TIK telah meningkatkan efektivitas operasional melalui sistem seperti *Battle Management System* (BMS), *Integrated Command and Control System* (ICCS), dan aplikasi pengelolaan data personel maupun logistik. Namun, tantangan yang dihadapi meliputi keterbatasan infrastruktur komunikasi jarak jauh, rendahnya integrasi sistem informasi, keterbatasan sumber daya manusia, serta ancaman keamanan siber. Perbandingan dengan praktik terbaik internasional menunjukkan adanya kesenjangan yang perlu diatasi melalui penguatan infrastruktur, integrasi sistem, peningkatan kapasitas SDM, dan kolaborasi internasional. Rekomendasi strategis meliputi pembangunan *backbone* komunikasi berkapasitas besar, peta jalan integrasi sistem, pelatihan berkelanjutan, perlindungan siber, dan diplomasi pertahanan berbasis TIK.

Kata kunci: Teknologi Informasi dan Komunikasi, TNI AD, Operasi Militer, *Network Centric Warfare*, Keamanan Siber.

PENDAHULUAN

Perkembangan pesat teknologi informasi dan komunikasi (TIK) telah membawa perubahan signifikan pada cara militer modern merencanakan, melaksanakan, dan mengevaluasi operasi. Dalam konteks TNI Angkatan Darat (TNI AD), TIK tidak hanya berperan sebagai alat bantu teknis, tetapi juga menjadi faktor strategis yang memengaruhi efektivitas, kecepatan pengambilan keputusan, dan keunggulan dalam operasi militer. TNI AD memanfaatkan inovasi TIK untuk meningkatkan efisiensi, efektivitas, dan daya tanggap operasionalnya. Teknologi ini memungkinkan koordinasi yang lebih baik antara unit TNI AD dan instansi sipil, sehingga memperkuat pertahanan negara secara keseluruhan. Dengan sistem komunikasi dan pengolahan data yang modern, proses pengambilan keputusan dapat berlangsung lebih cepat dan akurat. Oleh karena itu, modernisasi TIK di lingkungan TNI AD merupakan kebutuhan mendesak dalam menghadapi tantangan keamanan yang semakin kompleks (Rohman, 2023; TNI AD, 2019).

Salah satu perkembangan penting adalah konsep *Network Centric Warfare* (NCW), yang memanfaatkan TIK untuk menghubungkan unit militer yang tersebar secara geografis melalui sistem komunikasi terintegrasi. NCW memungkinkan peningkatan efektivitas tempur dan percepatan pengambilan keputusan strategis (Andrew, 2021; Sumari, 2007). Doktrin ini sejalan dengan Doktrin Lapangan Manajemen Informasi TNI AD, yang menekankan bahwa pertempuran modern membutuhkan keunggulan komunikasi dan informasi guna mendukung analisis intelijen, koordinasi operasi, mekanisme staf, serta optimalisasi sistem kesenjataan (TNI AD, 2019).

Namun, implementasi TIK di lingkungan TNI AD belum sepenuhnya optimal. Beberapa penelitian mengungkapkan adanya hambatan seperti keterbatasan infrastruktur jaringan komunikasi jarak jauh berkapasitas besar (Rohman, 2023; Triregina dkk., 2023), rendahnya integrasi antar sistem informasi (Udayana dkk., 2022), dan kesenjangan kompetensi sumber daya manusia dalam mengelola sistem NCW (Andrew, 2021). Kondisi ini menimbulkan kebutuhan mendesak untuk merumuskan strategi penguatan TIK yang terstruktur, terintegrasi, dan adaptif terhadap perkembangan ancaman modern, termasuk ancaman *hybrid warfare* (Asmoro dkk., 2021).

Berdasarkan konteks tersebut, penelitian ini dilakukan untuk mengkaji secara komprehensif implementasi TIK di TNI AD, termasuk kondisi aktual, manfaat, tantangan, dan prospek pengembangannya. Perbandingan dengan praktik terbaik negara lain seperti Amerika Serikat, Inggris, Jepang, dan Malaysia diharapkan dapat menjadi referensi strategis bagi peningkatan kapabilitas TIK militer Indonesia (Feakin dkk., 2014; Pakuningjati, 2018; Uren dkk., 2017).

Tujuan dari penelitian ini adalah:

1. Menganalisis kondisi terkini implementasi TIK di TNI AD beserta manfaatnya bagi operasi militer.
2. Mengidentifikasi tantangan yang dihadapi dalam pengembangan dan integrasi TIK.
3. Memberikan rekomendasi strategis untuk penguatan TIK di masa depan.

Dengan demikian, hasil kajian ini diharapkan dapat memberikan kontribusi bagi upaya modernisasi pertahanan nasional, sekaligus memperkuat peran TNI AD dalam menjaga keamanan dan kedaulatan negara di era digital.

METODE

Penelitian ini menggunakan pendekatan kualitatif berbasis studi literatur, dengan tujuan untuk memperoleh pemahaman mendalam mengenai implementasi teknologi informasi dan komunikasi (TIK) dalam mendukung operasional militer TNI AD. Metode ini dipilih karena memungkinkan eksplorasi berbagai aspek normatif, teknologis, dan kebijakan yang mendasari transformasi digital militer secara kontekstual.

Sumber data dalam penelitian ini terdiri dari:

1. Dokumen resmi TNI AD, seperti Doktrin Lapangan Manajemen Informasi (2019) dan Buku Petunjuk Induk tentang Perhubungan (2013).
2. Literatur akademik dan jurnal ilmiah yang relevan, baik nasional maupun internasional, yang terbit dalam rentang waktu 2007–2025, khususnya terkait implementasi NCW, interoperabilitas militer, dan kesiapan siber.
3. Laporan resmi dan data hasil litbanghan, termasuk presentasi internal dari Paban III/Litbang Asro Srenaad (2024).
4. Studi perbandingan dari negara-negara maju seperti Amerika Serikat dan Inggris, serta yang relatif di atas Indonesia seperti Jepang dan Malaysia sebagai *benchmark* internasional.

Kriteria pemilihan referensi didasarkan pada relevansi topik, keterbaruan (terutama pasca 2020), dan kontribusi pada kajian strategis TIK militer. Data dianalisis secara deskriptif-komparatif, dengan mengelompokkan informasi ke dalam empat kategori utama: kondisi aktual, manfaat, tantangan, dan prospek pengembangan TIK. Selanjutnya, dilakukan perbandingan antara kondisi TNI AD dan praktik terbaik internasional untuk mengidentifikasi kesenjangan serta menyusun rekomendasi strategis.

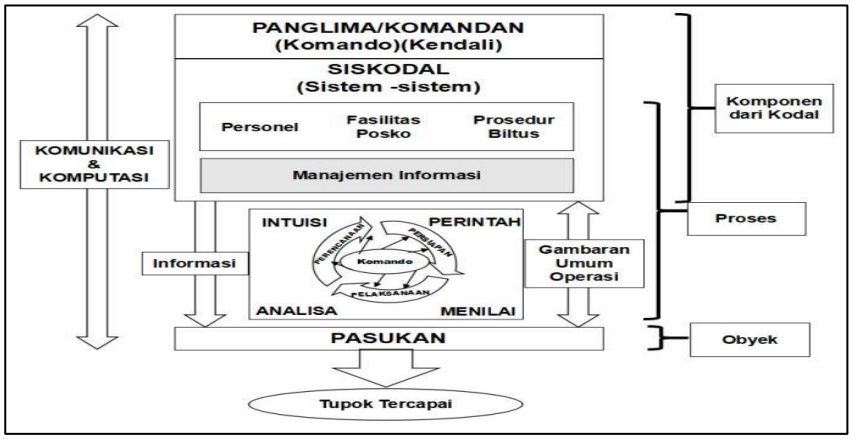
Batasan studi ini terletak pada ketergantungan terhadap sumber sekunder dan terbatasnya akses pada data operasional aktual yang bersifat rahasia militer. Meski demikian, triangulasi sumber dilakukan untuk menjaga validitas informasi dan menghindari bias interpretatif. Fokus artikel adalah pada TNI AD, sehingga temuan tidak secara langsung digeneralisasi ke matra lainnya.

HASIL

Implementasi TIK dalam Operasi Militer

Salah satu teknologi yang memiliki dampak besar dalam doktrin perang adalah teknologi informasi dan komunikasi (Rohman, 2023). Teknologi informasi dan komunikasi (TIK) memiliki peran strategis dalam mendukung operasi militer modern. Dalam Doktrin Lapangan Manajemen Informasi TNI AD (TNI AD, 2019) dijelaskan bahwa pertempuran masa kini dan masa depan membutuhkan keunggulan komunikasi dan informasi. Data yang akurat menjadi landasan bagi analisis intelijen, sistem komunikasi, koordinasi operasi, mekanisme staf, dan optimalisasi sistem kesenjataan.

Perkembangan konsep *Network Centric Warfare* (NCW) telah mendorong penggunaan TIK untuk menghubungkan unit militer yang tersebar secara geografis melalui sistem komunikasi terintegrasi, sehingga meningkatkan efektivitas tempur dan kecepatan pengambilan keputusan (Andrew, 2021). Visualisasi mekanisme manajemen informasi pada sistem Kodalops di TNI AD dapat dilihat pada Gambar 1.Terlihat jelas bahwa TIK berperan besar dalam manajemen informasi dalam Siskodalops TNI AD melalui komunikasi dan komputasi.



Gambar 1. Visualisasi mekanisme Manajemen Informasi pada Sistem Kodalops.
(Sumber: TNI AD (2019))

Kondisi Aktual TIK di TNI AD

Sistem informasi terdistribusi yang ada saat ini telah mendukung kolaborasi antar satuan TNI AD, namun penelitian menunjukkan bahwa jaringan sistem informasi tersebut masih belum terorganisir dengan baik dan kurang terintegrasi (Udayana dkk., 2022). Akibatnya, aliran informasi untuk operasi militer belum optimal, dan diperlukan peningkatan infrastruktur TIK agar visi keamanan nasional dapat tercapai (Bateman dkk., 2013).

Implementasi TIK di lingkungan TNI AD yang telah mendapat perhatian dari para peneliti antara lain:

1. Sistem informasi personel (Sisfopers) di Akademi Militer yang mempermudah pengelolaan data personel, meski masih menghadapi kendala pembaruan data tepat waktu (Sarwono & Assery, 2023). Secara lebih luas juga sudah tergelar Sisfopers TNI AD, Sisfolog TNI AD, Sisforen TNI AD, dan Sisfoharwat TNI AD (Mutaqin dkk., 2023).
2. *Integrated Command and Control System* (ICCS) yang menggunakan protokol komunikasi CY-16H/Link Kartika untuk menghubungkan unsur taktis dan strategis dalam peperangan berbasis jaringan (Rohman, 2023). Ini merupakan *Battle Management System* (BMS) hasil dari Litbanghan Pushubad (sekarang Puskomlekad) yang sudah diproduksi masal (Paban III/Litbang Asro Srenaad, 2024). Implementasi ICCS ini sejalan dengan rekomendasi Imasfy (2023) yang menekankan pentingnya interoperabilitas TIK antar-satuan di Matra Darat guna mendukung efektivitas NCW.

Meskipun demikian, hambatan utama yang dihadapi meliputi kurangnya infrastruktur *backbone* komunikasi data jarak jauh berkapasitas besar (Triregina dkk., 2023), keterbatasan integrasi antar sistem informasi (Udayana dkk., 2022), dan kesiapan sumber daya manusia (Andrew, 2021).

Evaluasi Infrastruktur TIK

Evaluasi kesiapan siber berdasarkan metrik yang digunakan oleh *Australian Strategic Policy Institute* (ASPI) menunjukkan peningkatan peran militer Indonesia dalam aspek pemanfaatan, kebijakan, dan keamanan siber selama periode 2014 hingga 2017. Pada tahun 2014, Indonesia memperoleh skor 4 dari 10, setara dengan India, Malaysia, dan Thailand. Posisi ini menempatkan Indonesia pada peringkat 11–14 dari 16 negara yang dianalisis, jauh di bawah Amerika Serikat (skor 9), serta Inggris dan Tiongkok (skor 8) yang menempati posisi atas (Feakin dkk., 2014) (Lihat Tabel 1).

NO/PERINGKAT	MILITER NEGARA	SKOR
1	Amerika Serikat	9
2-3	Inggris, Tiongkok	8
4-7	Australia, Korea Selatan, Singapura, Korea Utara	7
8	Jepang	6
9-10	Filipina, Myanmar	5
11-14	India, Indonesia, Malaysia, Thailand	4
15-16	Papua Nugini, Kamboja	2

Tabel 1. Skor Peran Militer Negara Asia Pasifik dalam Pemanfaatan, Kebijakan, dan Keamanan Siber di Negaranya (Tahun 2014).
(Data diolah kembali sesuai kebutuhan penyajian, dari sumber: Feakin dkk. (2014))

Namun, pada laporan edisi 2017, skor Indonesia meningkat menjadi 6 dari 10, menempatkannya di posisi 9 dari 25 negara Asia Pasifik. Peningkatan ini menunjukkan komitmen yang lebih kuat dalam pengembangan kapabilitas pertahanan siber, termasuk pembentukan satuan siber militer di bawah BAIS TNI dan pengakuan eksplisit terhadap ancaman siber dalam dokumen strategis pertahanan nasional. Meskipun begitu, Indonesia masih tertinggal dibanding Singapura dan Korea Selatan (skor 9), Australia, Tiongkok, dan Korea Utara (skor 8), serta Jepang dan Malaysia (skor 7) yang telah mengembangkan struktur dan doktrin pertahanan siber yang lebih mapan (Uren dkk., 2017) (Lihat Tabel 2).

NO/PERINGKAT	MILITER NEGARA	SKOR
1	Amerika Serikat	10
2-3	Singapura, Korea Selatan	9
4-6	Australia, Tiongkok, Korea Utara	8
7-8	Jepang, Malaysia	7
9	Indonesia	6
10-13	Myanmar, Selandia Baru, Taiwan, Thailand	5
14-15	Brunei, Pakistan	4
16-18	India, Filipina, Vietnam	3
19-23	Bangladesh, Kamboja, Fiji, Laos, Papua Nugini	1
24-25	Kepulauan Salomon, Vanuatu	0

Tabel 2. Skor Peran Militer Negara Asia Pasifik dalam Pemanfaatan, Kebijakan, dan Keamanan Siber di Negaranya (Tahun 2017).
(Data diolah kembali sesuai kebutuhan penyajian, dari sumber: Uren dkk. (2017))

Teknologi Utama yang Digunakan

TNI AD telah mengembangkan dan menggunakan berbagai alat dan sarana prasarana TIK modern, antara lain:

1. *Battle Management System* (BMS), hasil litbanghan Pushubad yang telah diproduksi massal (Gambar 2).
2. Sisfo Potensi Telekomunikasi (hasil litbanghan Pushubad) dan Posko Dahanud mobile (hasil litbanghan Pussenarhanud) untuk mendukung operasi pertahanan udara.
3. Teknologi keamanan siber untuk melindungi data strategis dari ancaman digital.

Gambar 2. *Battle Management System* (BMS), produk Litbanghan TNI AD yang sudah diproduksi masal sebagai salah satu implementasi TIK di TNI AD.
(Sumber: Paban III/Litbang Asro Srenaad 2024)

Manfaat Implementasi TIK

Pemanfaatan TIK di TNI AD memberikan berbagai manfaat, antara lain:

1. Peningkatan komunikasi dan koordinasi antar satuan, baik dalam operasi maupun latihan (Udayana dkk., 2022).
2. Efisiensi operasional, termasuk percepatan pengadaan dan distribusi logistik berbasis sistem manajemen digital.
3. Penguatan analisis data untuk pengambilan keputusan strategis yang lebih tepat, termasuk melalui penerapan kerangka Analisis Sistem dan Riset Operasi (ASRO) yang terintegrasi dengan TIK (Turnip, 2025).
4. Diplomasi pertahanan, melalui peningkatan kerja sama internasional yang difasilitasi oleh teknologi informasi (Bateman dkk., 2013; Taylor dkk., 2014).

Tantangan Implementasi TIK di TNI AD

Meskipun penerapan TIK di TNI AD telah memberikan manfaat signifikan, sejumlah tantangan masih menghambat optimalisasi pemanfaatannya. Tantangan-tantangan tersebut meliputi:

1. *Keterbatasan infrastruktur dan anggaran*.
   a. Infrastruktur *backbone* komunikasi data jarak jauh dengan kapasitas besar masih belum tersedia, dan kemungkinan memerlukan satelit khusus militer (Rohman, 2023; Triregina dkk., 2023).
   b. Keterbatasan anggaran menghambat pengembangan sistem informasi modern yang diperlukan (Bateman dkk., 2013).
   c. Data dari Srenaad menunjukkan bahwa dari 427 prototipe materiel hasil litbanghan selama 2006–2024 yang sebagian besar merupakan rekayasa dan pengembangan TIK, hanya 17 yang diproduksi massal (Paban III/Litbang Asro Srenaad, 2024).
2. *Kesiapan sumber daya manusia (SDM)*.

a. Masih terdapat kesenjangan keterampilan dalam mengoperasikan dan mengelola sistem NCW di kalangan personel (Andrew, 2021).
b. Adaptasi terhadap teknologi baru sering kali menghadapi resistensi dari personel yang lebih nyaman dengan metode lama.

3. *Ego sektoral dan koordinasi antar unit*. Tugas pengelolaan TIK di TNI AD secara teknis terbagi antara Disinfolahtad, Komlek (sebelumnya Perhubungan/Hub), dan Satuan Sandi dan Siber, yang berpotensi menimbulkan tumpang tindih fungsi (Mutaqin dkk., 2023; TNI AD, 2013).
4. *Keamanan siber*. Ancaman serangan siber terhadap infrastruktur militer semakin kompleks, sementara kapasitas pertahanan siber belum sepenuhnya setara dengan ancaman yang dihadapi (Rohman, 2023). Selain itu, Mutaqin dkk. (2024) mengingatkan bahwa perkembangan TIK yang pesat juga membawa risiko baru, termasuk potensi penyalahgunaan teknologi yang dapat berdampak pada kerahasiaan dan keamanan operasi militer. Kristian & Rochaeni (2022) juga menegaskan bahwa keunggulan dalam perang elektronika memerlukan tenaga kerja pasukan siber yang terlatih, kemampuan intelijen siber yang mumpuni, dan organisasi kekuatan siber yang terstruktur dalam format jaringan untuk berbagi informasi secara *real-time*.

PEMBAHASAN

Hasil kajian menunjukkan bahwa teknologi informasi dan komunikasi (TIK) memiliki peran strategis dalam meningkatkan efektivitas operasional dan strategis TNI AD. Penerapan sistem seperti *Battle Management System* (BMS), *Integrated Command and Control System* (ICCS), dan Sisfopers maupun Sisfo lainnya termasuk Sisfolog telah memberikan kontribusi nyata terhadap kecepatan koordinasi, akurasi informasi, dan efisiensi operasional. Temuan ini sejalan dengan pendapat Rohman (2023) dan Andrew (2021) yang menegaskan bahwa penguasaan TIK, khususnya dalam konsep *Network Centric Warfare* (NCW), menjadi kunci bagi superioritas militer modern. Sejumlah studi menunjukkan bahwa integrasi sistem informasi dengan kerangka analisis operasional mampu meningkatkan efektivitas pengambilan keputusan militer secara signifikan (Alberts dkk., 1999; Imasfy, 2023; Rohman, 2023). Dalam konteks ini, Turnip (2025) mengembangkan pendekatan Analisis Sistem dan Riset Operasi (ASRO) sebagai model terapan untuk TNI AD, yang mendukung optimalisasi logistik dan mitigasi risiko operasional melalui pemrosesan informasi yang lebih adaptif. Pendekatan ini sejalan dengan strategi penguatan sistem pengambilan keputusan berbasis NCW yang diuraikan oleh Rohman (2023), serta gagasan interoperabilitas sistem komando di lingkungan matra darat sebagaimana dikembangkan oleh Imasfy (2023).

Meskipun demikian, kesenjangan infrastruktur, integrasi sistem yang belum optimal, dan keterbatasan kapasitas sumber daya manusia (SDM) menunjukkan bahwa penerapan TIK di TNI AD belum sepenuhnya mencapai standar negara-negara maju. Laporan *Cyber Maturity in the Asia–Pacific Region* oleh ASPI menunjukkan bahwa pada tahun 2014, Indonesia memperoleh skor 4 dari 10 dalam kesiapan siber militer, setara dengan India, Malaysia, dan Thailand, jauh di bawah Amerika Serikat (skor 9) serta Inggris dan Tiongkok (skor 8) (Feakin dkk., 2014). Pada tahun 2017, skor Indonesia meningkat menjadi 6, menandai kemajuan dalam pengembangan kapabilitas pertahanan siber, termasuk pembentukan satuan siber dan penyusunan kebijakan strategis. Namun, posisi tersebut masih berada di bawah negara-negara seperti Singapura dan Korea Selatan (skor 9), serta Australia dan Tiongkok (skor 8), yang telah mengintegrasikan doktrin, kelembagaan, dan sumber daya secara lebih komprehensif (Uren dkk., 2017).

Uren dkk. (2017) juga mencatat adanya arahan TNI kepada prajurit terkait ancaman *cyber narcoterrorism* dan penyebaran berita palsu. TNI telah membentuk badan siber yang mencakup fungsi pelacakan rudal dan pengawasan satelit, sementara masing-masing matra mempertimbangkan pembentukan unit khusus siber. Meski pada 2016 terjadi kemajuan signifikan dalam penataan peran ini, perkembangan berikutnya relatif stagnan. Pentingnya klarifikasi peran dalam pertahanan jaringan, operasi ofensif, dan peningkatan kesadaran terhadap kerentanan ancaman siber pun menjadi sorotan. Hingga kini, isu siber di lingkungan TNI kerap diposisikan sebagai bidang khusus dalam kerangka peperangan elektronik dan informasi. Hal ini mengindikasikan bahwa Indonesia masih memerlukan upaya berkelanjutan untuk memperkuat kebijakan, infrastruktur, serta kualitas dan kuantitas SDM di bidang pertahanan siber.

Sebagai perbandingan, Jepang dan Malaysia, dua negara dengan skor satu tingkat di atas Indonesia sesuai penilaian dan observasi Uren dkk. pada tahun 2017, menunjukkan pendekatan yang berbeda dalam memperkuat peran militer di ranah siber. Di Jepang, *Ministry of Defense Cyber Defence Unit* yang awalnya hanya beranggotakan sekitar 90 personel, bertugas melindungi instalasi militer, kementerian, dan infrastruktur kritis. Pemerintah berencana meningkatkan jumlah personel menjadi sekitar 1.000 orang dan membentuk kelompok kerja khusus untuk mempelajari teknik cyberwarfare, terutama menjelang Olimpiade Tokyo 2020. Tantangan Jepang adalah keterbatasan yang diakibatkan konstitusi pasifis dan klasifikasi serangan siber sebagai tindak pidana, bukan aksi perang, sehingga diperlukan doktrin yang lebih jelas terkait penggunaan ranah siber dalam operasi militer.

Sementara itu, Malaysia meningkatkan kesadaran dan kemampuan pertahanan siber militernya melalui *Armed Forces Cyber Defence Operations Centre* yang resmi beroperasi pada September 2017 setelah sembilan bulan pengujian. Pusat ini membantu pelatihan teknis dan menjadi tulang punggung peningkatan kapabilitas operasi siber militer. Dukungan kebijakan yang jelas dari Kementerian Pertahanan, serta integrasi dalam *National Defence Policy*, memperkuat fondasi strategis pertahanan siber Malaysia.

Perbandingan dengan praktik internasional memperlihatkan perbedaan yang cukup jelas. Amerika Serikat, misalnya, telah mengintegrasikan NCW secara menyeluruh, memanfaatkan TIK untuk menghubungkan berbagai elemen militer dalam satu jaringan terpadu (*real-time data sharing*), yang berdampak pada percepatan pengambilan keputusan dan peningkatan efektivitas tempur (Sumari, 2007). Inggris, di sisi lain, memperkuat pertahanan siber melalui strategi komprehensif 2016–2021 yang mencakup pertahanan, pencegahan, pengembangan kapabilitas, dan kerja sama internasional (Pakuningjati, 2018).

Dalam konteks Indonesia, tantangan penerapan TIK juga terkait erat dengan faktor struktural organisasi. Seperti diungkapkan Mutaqin dkk. (2023), pembagian peran antara Disinfolahtad, Komlek, dan Satuan Sandi dan Siber seringkali berpotensi menimbulkan tumpang tindih fungsi. Kondisi ini dapat memperlambat pengambilan keputusan strategis dan menghambat implementasi teknologi baru. Oleh karena itu, diperlukan sinergi antar unit, yang dapat difasilitasi melalui peta jalan pengembangan TIK terintegrasi dan kebijakan yang mengedepankan kolaborasi. Rekomendasi pembentukan satuan tempur siber khusus, seperti Batalyon Perang Elektronika di bawah Puskomlek TNI AD (sebelumnya Pushubad), sebagaimana diusulkan Kristian & Rochaeni (2022), selaras dengan kebutuhan reformasi organisasi TNI AD di bidang TIK.

Selain aspek teknis dan organisasi, faktor sumber daya manusia menjadi kunci keberhasilan. Andrew (2021) menyoroti bahwa kesiapan personel dalam mengoperasikan sistem NCW menjadi kendala utama dalam penerapannya secara efektif. Konsep *The Strategic Corporal*, pertama kali diperkenalkan oleh Krulak (1999), menekankan

pentingnya kewenangan pengambilan keputusan oleh prajurit tingkat bawah dalam situasi kompleks yang menuntut respons cepat dan berbasis informasi. Dalam konteks TNI AD, Turnip (2024) mengadaptasi konsep ini dengan menekankan bahwa keberhasilan implementasi TIK dapat meningkatkan *situational awareness* dan efektivitas komando-kendali di tingkat satuan bawah. Hal ini juga sejalan dengan temuan Imasfy (2023) yang menekankan bahwa interoperabilitas TIK dalam NCW Matra Darat memerlukan arsitektur sistem informasi yang terintegrasi dan dapat beroperasi secara *real-time* di berbagai level satuan. Rohman (2023) turut menggarisbawahi pentingnya transformasi digital berbasis infrastruktur komunikasi dan kesiapan SDM sebagai fondasi keberhasilan pengambilan keputusan yang desentralistik dan responsif di lingkungan TNI. Penelitian Laksmana (2019) juga mengindikasikan bahwa keterampilan adaptasi terhadap model teknologi asing dapat menentukan keberhasilan integrasi teknologi baru. Pelatihan berkelanjutan dan peningkatan literasi digital di semua level komando TNI AD akan sangat menentukan keberhasilan transformasi ini.

Di sisi lain, manfaat strategis TIK tidak hanya terbatas pada internal TNI AD. Seperti diuraikan Bateman dkk. (2013) dan Taylor dkk. (2014), TIK juga mendukung diplomasi pertahanan melalui peningkatan interoperabilitas dengan militer negara sahabat, pertukaran informasi yang lebih cepat, dan koordinasi multilateral. Dalam konteks keamanan regional, interoperabilitas berbasis satelit (Triregina dkk., 2023) dapat menjadi solusi untuk memperkuat pertahanan perbatasan dan keamanan maritim Indonesia. Selain itu, Asmoro dkk. (2021) menekankan bahwa penguatan organisasi dan doktrin pertahanan negara menjadi langkah strategis yang tidak terpisahkan dalam menghadapi ancaman *hybrid warfare*. Implementasi TIK di lingkungan TNI AD perlu selaras dengan penataan doktrin tersebut, sehingga setiap inovasi teknologi memiliki kesesuaian langsung dengan kebutuhan pertahanan adaptif.

Dengan mempertimbangkan keseluruhan temuan ini, dapat disimpulkan bahwa keberhasilan transformasi digital di TNI AD memerlukan kombinasi peningkatan infrastruktur, integrasi sistem, penguatan SDM, dan reformasi organisasi. Langkah-langkah tersebut akan memosisikan TNI AD pada jalur yang tepat untuk mencapai keunggulan operasional di era peperangan berbasis informasi.

Kontribusi teoritis dari penelitian ini terletak pada integrasi konsep *Network Centric Warfare* (NCW) dengan pendekatan Analisis Sistem dan Riset Operasi (ASRO) dalam konteks pengembangan teknologi informasi dan komunikasi (TIK) di militer negara berkembang. Dengan menggabungkan kerangka konseptual ini, artikel ini menawarkan model pemahaman baru tentang bagaimana TIK tidak hanya menjadi instrumen teknis, tetapi juga sebagai pengungkit strategi komando, pengambilan keputusan, dan interoperabilitas dalam sistem pertahanan darat. Model ini dapat dikembangkan lebih lanjut sebagai landasan untuk studi kebijakan pertahanan berbasis teknologi, khususnya dalam menilai kesiapan digital militer secara menyeluruh di tingkat taktis dan strategis. Dengan demikian, penelitian ini memberikan kontribusi terhadap literatur strategis militer dengan menawarkan perspektif adaptif berbasis konteks Indonesia, yang relevan bagi studi keamanan dan pertahanan di kawasan.

KESIMPULAN DAN REKOMENDASI

Kesimpulan

1. *Peran strategis TIK dalam operasi militer*. Penerapan teknologi informasi dan komunikasi (TIK) di TNI AD telah memberikan kontribusi signifikan terhadap peningkatan efektivitas strategis dan operasional. Sistem seperti *Battle Management System* (BMS),

Integrated Command and Control System (ICCS), dan berbagai aplikasi pengelolaan data telah mempercepat koordinasi, meningkatkan akurasi informasi, dan mempersingkat proses pengambilan keputusan.

2. *Kondisi aktual dan kesenjangan*. Meskipun kemajuan telah dicapai, kondisi TIK di TNI AD masih menghadapi kendala serius, antara lain keterbatasan infrastruktur *backbone* komunikasi jarak jauh, rendahnya integrasi sistem informasi, keterbatasan kesiapan SDM, dan ancaman keamanan siber yang terus berkembang.
3. *Perbandingan dengan praktik terbaik internasional*. Dibandingkan dengan negara maju seperti Amerika Serikat dan Inggris, serta negara yang relatif satu tingkat di atas Indonesia seperti Jepang dan Malaysia, penerapan TIK di TNI AD masih tertinggal, terutama dalam hal integrasi sistem, kesiapan siber, dan pengembangan interoperabilitas.
4. *Implikasi strategis*. Keberhasilan transformasi digital di TNI AD tidak hanya berpengaruh pada peningkatan kemampuan tempur, tetapi juga memperkuat diplomasi pertahanan dan kerja sama internasional. Peningkatan interoperabilitas, khususnya berbasis satelit, dapat mendukung keamanan perbatasan dan maritim.

Rekomendasi

1. *Penguatan infrastruktur TIK.*
   a. Membangun *backbone* komunikasi data jarak jauh berkapasitas besar, termasuk opsi satelit khusus militer untuk mendukung operasi di seluruh wilayah Indonesia.
   b. Memperluas cakupan jaringan komunikasi aman untuk menghubungkan semua satuan secara *real-time*.
2. *Integrasi sistem informasi.*
   a. Menyusun peta jalan pengembangan sistem informasi terintegrasi yang menghubungkan seluruh satuan dan fungsi di TNI AD.
   b. Mengurangi ego sektoral antar unit pengelola TIK (Disinfolahtad, Komlek, Satuan Sandi dan Siber) melalui kebijakan koordinasi terpadu.
3. *Penguatan sumber daya manusia.*
   a. Menyelenggarakan pelatihan berkelanjutan bagi personel di semua level komando terkait operasi sistem NCW, keamanan siber, dan manajemen data.
   b. Mengadopsi praktik pelatihan adaptif dari mitra internasional untuk mempercepat peningkatan kompetensi.
4. *Perlindungan keamanan siber.*
   a. Meningkatkan kemampuan pertahanan siber untuk melindungi infrastruktur strategis dari ancaman serangan digital.
   b. Menerapkan sistem deteksi dini dan respons cepat terhadap ancaman siber.
5. *Kolaborasi dan diplomasi pertahanan.*
   a. Memperkuat kerja sama internasional dalam bidang TIK militer, termasuk pertukaran teknologi, interoperabilitas, dan latihan gabungan.
   b. Mengoptimalkan peran TIK sebagai sarana diplomasi pertahanan untuk membangun kepercayaan di tingkat regional.

REFERENSI

Alberts, D. S., Garstka, J. J., & Stein, F. P. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority* (2nd Ed (Revised)). CCRP. https://apps.dtic.mil/sti/tr/pdf/ADA406255.pdf

Andrew, T. (2021). Network Centric Warfare sebagai Upaya Transformasi Perang TNI. *Defendonesia*, *5*(1), 35–45. https://doi.org/10.54755/defendonesia.v5i1.101

Asmoro, N., Sutomo, A., Haryono, T., & Putri, R. (2021). The Structuring of Organizational and Doctrine of State Defense in Facing Hybrid Warfare. *Jurnal Pertahanan: Media Informasi ttg Kajian & Strategi Pertahanan yang Mengedepankan Identity, Nasionalism & Integrity*, *7*(2), 309–319. https://doi.org/10.33172/jp.v7i2.1220

Bateman, S., Bergin, A., & Channer, H. (2013). *Terms of Engagement: Australia's Regional Defence Diplomacy*. https://apo.org.au/node/34931

Feakin, T., Woodall, J., & Aiken, K. (2014). *Cyber Maturity in the Asia-Pacific Region 2014*. The Australian Strategic Policy Institute Limited. https://core.ac.uk/download/pdf/30674827.pdf

Imasfy, M. (2023). Strategi Interoperabilitas Pemanfaatan Teknologi Informasi dan Komunikasi (TIK) dalam Mendukung Network Centric Warfare (NCW) Matra Darat. *Jurnal Strategi Pertahanan Darat (JSPD)*, *9*(1). https://doi.org/10.33172/jspd.v9i1.11155

Kristian, I., & Rochaeni, A. (2022). Strategi Militer Mengenai Siber untuk Keunggulan Dunia Maya dalam Perang Elektronik. *Jurnal Caraka Prabu*, *6*(2), 207–2016. https://doi.org/10.36859/jcp.v6i2.1176

Krulak, C. C. (1999). The Strategic Corporal: Leadership in the Three Block War. *Marine Corps Gazette & Leatherneck Magazine of the Marines, January 1999*, *82*(1), 14–17. https://www.mca-marines.org/wp-content/uploads/1999-Jan-The-strategic-corporal-Leadership-in-the-three-block-war.pdf

Laksmana, E. A. (2019). *Imitation Game: Military Institutions and Westernization in Indonesia and Japan* [Doctoral Dissertation, Syracuse University]. https://surface.syr.edu/etd/1126

Mutaqin, R., Mutaqin, G., & Dharmopadni, D. S. (2024). Dampak Perkembangan Teknologi Informasi dan Komunikasi terhadap Dinas Militer. *Jurnal Ilmiah Multidisiplin*, *2*(3), 199–04. https://doi.org/10.59000/jim.v2i3.213

Mutaqin, R., Sahary, F. T., Mutaqin, G., & Dharmopadni, D. S. (2023). Peran Disinfolahtad dalam Mempercepat Transformasi Digital di Lingkungan TNI AD. *Jurnal Academia Praja*, *6*(2), 229–244. https://doi.org/10.36859/jap.v6i2.1732

Paban III/Litbang Asro Srenaad. (2024). Regulasi dan Kebijakan Litbanghan TNI AD. Dalam *Presentasi pada Verifikasi Kapabilitas Industri Pertahanan dalam Mendukung Litbanghan TNI AD, Arya Duta Hotel, Menteng, Jakarta, 2024*.

Pakuningjati, A. L. (2018). *Merefleksi Strategi Keamanan Siber Nasional Inggris 2016-2021*. https://cfds.fisipol.ugm.ac.id/wp-content/uploads/sites/1423/2021/01/41-CfDS-Case-Study-Merefleksi-Strategi-Keamanan-Siber-Nasional-Inggris-2016-2021.pdf

Rohman, M. (2023). *Optimalisasi Transformasi Digital dalam Pembangunan NCW (Network Centric Warfare) TNI dalam rangka Ketahanan Nasional* [Taskap PPRA Lemhanas RI, Lemhanas RI]. http://lib.lemhannas.go.id/public/media/catalog/0010-112300000000071/swf/7409/PPRA%20LXV%2059%20-%202023.pdf

Sarwono, I., & Assery, S. (2023). Analisis Implementasi Sistem Informasi Personel di Akademi Militer. *Jurnal Riset Akuntansi dan Bisnis Indonesia*, *3*(3), 796–808. https://doi.org/10.32477/jrabi.v3i3.791

Sumari, A. D. W. (2007, Oktober). Network-Centric Warfare: Doktrin Tempur Era Informasi. *Satria Studi Pertahanan*, *3*(4), 90–103. https://www.researchgate.net/publication/330349084

Taylor, B., Blaxland, J., White, H., Bisley, N., Leahy, P., & Tan, S. S. (2014). *Defence Diplomacy Is the game worth the candle? Vol. CoG series paper #17* (A. Carr, Ed.). ANU Strategic and Defence Studies Centre. https://apo.org.au/node/42190

TNI AD. (2013). Buku Petunjuk Induk tentang Perhubungan. Dalam *Publikasi Internal TNI AD*. Markas Besar TNI AD.

TNI AD. (2019). Doktrin Lapangan Manajemen Informasi. Dalam *Publikasi Internal TNI AD*. Markas Besar TNI AD.

Triregina, I., Supriyadi, A. A., & Gultom, R. A. G. (2023). The Need for Satellite-Based Interoperability to Strengthen Maritime Security: A Study of Indonesian Border Defense. *International Journal of Progressive Sciences and Technologies (IJPSAT)*, *37*(1), 232–239. https://ijpsat.org/index.php/ijpsat/article/download/5053/3145

Turnip, H. M. S. (2024). The Strategic Corporal: Relevansinya bagi TNI AD. *Jipolis: Jurnal ilmu Politik dan Ilmu-ilmu Sosial*, *1*(3), 1–10. https://ejournal.fisip.unjani.ac.id/index.php/jipolis/article/view/3441

Turnip, H. M. S. (2025). Peran Analisis Sistem dan Riset Operasi (ASRO) dalam Strategi Militer Modern dan Optimasi Logistik. *Jurnal Elektrosista*, *12*(2), 103–122. https://ojs.akmil.ac.id/index.php/jurnal-elektrosista/article/view/322

Udayana, P. A., Legionosukmo, T., & Sundari, S. (2022). Strategy for Integrated Land Information System Network Arrangements for the Indonesian National Army. *Strategi Pertahanan Darat (JSPD)*, *8*(1). https://doi.org/10.33172/jspd.v8i1.1054

Uren, T., Hanson, F., Ryan, F., Chi, M., & Viola, J. (2017). *Cyber Maturity in the Asia-Pacific Region 2017*. The Australian Strategic Policy Institute Limited. https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017/