Jurnal Strategi Kampanye Militer
Volume 11, Nomor 1, 2025 E-ISSN 2830-3261

Pengembangan Strategis Sistem Informasi Personel Tentara Nasional Indonesia Berbasis Teknologi Informasi untuk Mendukung Kampanye Militer

Strategic Development of the Indonesian Armed Forces Personnel Information System Based on Information Technology to Support Military Campaigns

Efrizalsyah, Samsul Bahari, Erry Herman
Prodi Strategi dan Kampanye Militer,
Fakultas Strategi Pertahanan Unhan RI
Email: efrizalsyah160@gmail.com

Abstract. *The transformation of warfare in the 21st century has shifted toward asymmetric, hybrid, and cyber domains, where information technology (IT) plays a decisive role in determining military superiority. This study aims to formulate a strategic model for developing the Indonesian National Armed Forces (Tentara Nasional Indonesia—TNI) personnel information system based on IT integration to support military campaigns. Using a qualitative-evaluative approach combined with SWOT and Fishbone analyses, the research identifies three major challenges: the lack of infrastructure and inter-service integration, low digital competence among personnel, and the absence of standardized IT-based personnel management. Findings reveal that current TNI systems are only 65% digitally integrated, with significant operational inefficiencies in troop deployment and data synchronization during joint operations. The study recommends a comprehensive strategy comprising the adoption of Artificial Intelligence (AI), Big Data analytics, and cloud computing, accompanied by intensive personnel training and ISO/IEC 27001-based data security standardization. These measures will enhance interoperability, strengthen cyber resilience, and improve Command and Control (C2) efficiency. The results contribute to the modernization of Indonesia's defense human resource management and provide a policy framework for strengthening military readiness in the digital era.*

Keywords: *Military digitalization, personnel management, interoperability, cybersecurity, TNI, defense modernization.*

Abstrak. Transformasi karakter peperangan pada abad ke-21 telah bergeser ke arah domain asimetris, hibrida, dan siber, di mana teknologi informasi (TI) memainkan peran yang menentukan dalam menegakkan superioritas militer. Penelitian ini bertujuan untuk merumuskan model strategis pengembangan sistem informasi personel Tentara Nasional Indonesia (TNI) berbasis integrasi TI guna mendukung keberhasilan kampanye militer. Dengan menggunakan pendekatan kualitatif-

evaluatif yang dipadukan dengan analisis SWOT dan Fishbone, penelitian ini mengidentifikasi tiga tantangan utama, yaitu keterbatasan infrastruktur dan integrasi antarmatra, rendahnya kompetensi digital personel, serta belum adanya standar baku dalam pengelolaan personel berbasis TI. Temuan penelitian menunjukkan bahwa sistem informasi personel TNI saat ini baru mencapai tingkat integrasi digital sebesar 65%, sehingga masih terdapat berbagai ketidakefisienan operasional dalam penempatan pasukan dan sinkronisasi data selama operasi gabungan. Penelitian ini merekomendasikan strategi komprehensif yang meliputi penerapan *Artificial Intelligence (AI)*, analitik *Big Data*, dan *cloud computing*, yang disertai dengan pelatihan intensif bagi personel serta standarisasi keamanan data berdasarkan ISO/IEC 27001. Implementasi langkah-langkah tersebut diharapkan dapat meningkatkan interoperabilitas, memperkuat ketahanan siber, serta mengoptimalkan efektivitas *Command and Control (C2)*. Hasil penelitian ini berkontribusi terhadap modernisasi manajemen sumber daya manusia pertahanan Indonesia dan memberikan kerangka kebijakan bagi penguatan kesiapsiagaan militer di era digital.

Kata kunci: Digitalisasi militer, manajemen personel, interoperabilitas, keamanan siber, TNI, modernisasi pertahanan.

1. Pendahuluan.

Lingkungan keamanan global kontemporer ditandai oleh perkembangan teknologi yang sangat cepat serta munculnya bentuk konflik hibrida yang memadukan dimensi kinetik, informasi, dan siber (Gray, 1999). Dalam konteks ini, peperangan modern semakin didominasi oleh pengambilan keputusan berbasis data, intelijen waktu nyata, serta sistem pertahanan otomatis yang berlandaskan pada teknologi informasi. Kekuatan militer yang maju menyadari bahwa kemenangan di medan perang tidak lagi hanya ditentukan oleh kekuatan senjata, tetapi juga oleh keunggulan sistem informasi dan manajemen personel yang terintegrasi dalam jaringan digital yang terpadu. Departemen Pertahanan Amerika Serikat (U.S. Department of Defense/DoD) misalnya, mengembangkan *Defense Manpower Data Center* (DMDC), yakni platform terpusat yang mengintegrasikan kecerdasan buatan (*Artificial Intelligence/AI*) dan *Big Data* untuk mendukung kesiapan personel serta pengambilan keputusan dalam penempatan antar matra (U.S. DoD, 2022). Demikian

pula, Tentara Pembebasan Rakyat Tiongkok (*People's Liberation Army/PLA*) telah menggunakan sistem sumber daya manusia berbasis *cloud* yang menggabungkan pelatihan digital, pemantauan personel secara waktu nyata, serta kemampuan pertahanan siber (Tai, 2013). Sementara itu, *North Atlantic Treaty Organization* (NATO) mengoperasikan *Joint Personnel Management System* (JPMS) untuk menyelaraskan data di antara angkatan bersenjata multinasional guna memastikan interoperabilitas operasional dan struktur komando yang terpadu (NATO, 2019).

Berbeda dengan itu, Tentara Nasional Indonesia (TNI) masih menghadapi tantangan besar dalam membangun sistem terintegrasi yang sebanding. Saat ini, sekitar 65 persen sistem manajemen informasi personel TNI telah terdigitalisasi, namun sekitar 35 persen lainnya masih bergantung pada proses administrasi konvensional (Kementerian Pertahanan RI, 2023). Kondisi ini menghambat koordinasi antara TNI Angkatan Darat, TNI Angkatan Laut, dan TNI Angkatan Udara, terutama dalam pelaksanaan operasi militer gabungan di wilayah kompleks seperti Papua dan perbatasan Kalimantan. Dalam beberapa kasus, keterlambatan rotasi pasukan dan ketidaktepatan penempatan personel terjadi akibat ketidaksinkronan data antar matra.

Dari hasil kajian, muncul tiga persoalan utama dalam proses transformasi digital manajemen sumber daya manusia pertahanan di Indonesia. Pertama, keterbatasan infrastruktur dan lemahnya integrasi sistem yang menghambat pertukaran informasi secara waktu nyata antar matra. Pusat komando kerap bergantung pada data personel yang parsial atau usang sehingga menurunkan kecepatan respons dalam kampanye militer gabungan. Kedua, rendahnya kompetensi digital di kalangan personel. Berdasarkan data Komando Pendidikan dan Pelatihan TNI (Diklat TNI, 2023), hanya sekitar 40 persen personel yang memiliki literasi digital memadai untuk mengelola sistem berbasis data. Kesenjangan keterampilan ini menyebabkan ketidakefisienan dalam input data, miskomunikasi, dan keterlambatan proses administrasi. Ketiga, kurangnya interoperabilitas dan standarisasi antar sistem. Setiap matra TNI masih

mengoperasikan aplikasi manajemen personel sendiri tanpa kerangka keamanan atau basis data yang seragam. Akibatnya, hingga 45 persen data personel tidak dapat diakses secara lintas matra (Spers Mabes TNI, 2022). Fragmentasi ini melemahkan efektivitas *Command and Control* (C2) dan menjadi risiko strategis dalam lingkungan peperangan modern yang berbasis teknologi.

Tantangan tersebut mencerminkan dinamika transisi struktural yang kini dihadapi oleh banyak militer di negara berkembang—yakni upaya menyeimbangkan antara tradisi kelembagaan dengan tuntutan transformasi digital. Dalam konteks Indonesia, persoalan ini tidak semata bersifat administratif, tetapi juga strategis, karena berimplikasi langsung terhadap kesiapan operasional, mobilitas pasukan, serta kredibilitas pertahanan nasional.

Penelitian ini bertujuan merumuskan kerangka strategis pengembangan sistem informasi personel TNI berbasis integrasi teknologi informasi guna mendukung pelaksanaan kampanye militer. Secara khusus, penelitian ini menganalisis struktur dan tantangan aktual sistem informasi personel TNI, mengidentifikasi faktor teknologi, organisasi, dan sumber daya manusia yang memengaruhi interoperabilitas serta efektivitasnya, serta mengusulkan model komprehensif yang mengintegrasikan teknologi AI, *Big Data*, dan *cloud computing* untuk meningkatkan pengambilan keputusan berbasis data dalam operasi militer.

Secara teoretis, penelitian ini memberikan kontribusi terhadap *System Theory* (Bertalanffy, 1968; Ackoff, 1974) dengan menunjukkan bahwa ekosistem digital yang terintegrasi mampu memperkuat koordinasi organisasi dalam institusi pertahanan. Kajian ini juga memperkaya literatur mengenai *Military Human Resource Management* (Ulrich, 1997; Armstrong, 2014) dengan menyoroti hubungan antara pengembangan personel dan transformasi digital. Dalam konteks *Digital Defense Governance*, penelitian ini menawarkan model yang mengaitkan kesiapan sumber daya manusia dengan agenda modernisasi pertahanan Indonesia sebagaimana tertuang dalam

Undang-Undang Nomor 3 Tahun 2025 tentang Tentara Nasional Indonesia serta Peraturan Pemerintah Nomor 39 Tahun 2010 tentang Administrasi Personel Militer.

Secara praktis, model yang diusulkan menyediakan peta jalan strategis bagi para pembuat kebijakan dan perencana pertahanan untuk mengoptimalkan kesiapan personel melalui sistem digital yang terintegrasi. Penguatan manajemen personel berbasis TI tidak hanya akan meningkatkan efektivitas C2 TNI, tetapi juga memperkuat ketahanan nasional Indonesia dalam menghadapi tantangan peperangan hibrida dan siber pada abad ke-21.

2. Tinjauan Literatur

Kajian teoretis dalam penelitian ini berlandaskan pada *System Theory* yang dikembangkan oleh Ludwig von Bertalanffy (1968), yang memandang organisasi sebagai suatu sistem kompleks yang terdiri atas komponen-komponen yang saling berhubungan dan saling bergantung. Setiap subsistem berinteraksi secara dinamis dalam suatu struktur yang lebih luas untuk mencapai tujuan bersama. Dalam konteks lembaga pertahanan, sistem manajemen personel berfungsi sebagai subsistem vital yang menopang strategi militer secara keseluruhan. Pemikiran ini kemudian diperluas oleh Russell Ackoff (1974) yang menekankan bahwa efektivitas organisasi tidak ditentukan oleh kinerja masing-masing komponennya secara terpisah, tetapi oleh tingkat koordinasi dan sinergi di antara komponen tersebut. Peter Checkland (1981) melalui *Soft Systems Methodology* menambahkan dimensi sosial-teknologis dengan menegaskan bahwa unsur manusia, teknologi, dan prosedur dalam organisasi saling berinteraksi dalam lingkungan sosio-teknikal yang menuntut pemahaman holistik dan kemampuan adaptif. Dalam konteks Tentara Nasional Indonesia (TNI), sistem informasi personel dapat dipandang sebagai penghubung struktural antara fungsi pembinaan personel (Binpers) dan struktur komando operasional (*Command and Control – C2*). Fragmentasi sistem di antara matra darat, laut, dan udara mengurangi kemampuan TNI untuk memberikan respons terpadu dalam operasi

gabungan. Oleh karena itu, integrasi digital menjadi keharusan strategis guna menjamin interoperabilitas, akurasi data, dan kecepatan pengambilan keputusan, sesuai prinsip interdependensi sistemik sebagaimana ditegaskan oleh Gharajedaghi (2011) bahwa organisasi berbasis sistem hanya akan berfungsi optimal apabila dirancang secara sadar dan terarah—sebuah paradigma yang krusial dalam modernisasi institusi pertahanan di era digital.

Secara konseptual, penelitian ini juga menggunakan teori ancaman (*Threat Theory*) yang dikemukakan oleh Stephen M. Walt (1987) dalam kerangka *Balance of Threat*. Walt menjelaskan bahwa strategi pertahanan suatu negara tidak hanya dibentuk oleh besarnya kekuatan militer, tetapi juga oleh persepsi terhadap ancaman yang bersumber dari kapabilitas, kedekatan geografis, dan intensi lawan. Dalam konteks organisasi militer, logika ini diperluas menjadi kebutuhan untuk membangun kesiapan sumber daya manusia dan sistem informasi sebagai elemen utama dalam ketahanan strategis. Bagi TNI, modernisasi sistem informasi personel merupakan bentuk adaptasi kelembagaan terhadap perubahan karakter peperangan, di mana ancaman digital dan siber kini memiliki dampak strategis setara dengan ancaman konvensional. Seperti diuraikan oleh Nugroho (2023), persepsi ancaman dalam pertahanan modern mencakup kerentanan terhadap serangan siber, manipulasi data, serta perang informasi. Dengan demikian, *Threat Theory* memberikan dasar konseptual bagi upaya TNI untuk mengintegrasikan sistem personel lintas matra, sehingga kesiapan tidak hanya mencakup kekuatan fisik, tetapi juga ketahanan dalam domain informasi.

Selain itu, teori *Human Resource Management (HRM)* menjadi pilar menengah yang penting dalam penelitian ini. Dave Ulrich (1997), Michael Armstrong (2014), dan Gary Dessler (2019) menekankan bahwa manajemen sumber daya manusia modern tidak sekadar menjalankan fungsi administratif, melainkan menjadi mitra strategis organisasi. Ulrich menyoroti pentingnya penggunaan teknologi dan analitik dalam menciptakan nilai strategis, sedangkan Armstrong menekankan fungsi *Human*

Resource Information Systems (HRIS) dalam meningkatkan akurasi data, efisiensi kerja, dan pengambilan keputusan berbasis bukti (*evidence-based decision-making*). Dalam konteks militer, teori HRM perlu disesuaikan dengan karakteristik unik organisasi yang menjunjung disiplin, hierarki, serta kebutuhan akan respons cepat. Integrasi sistem HR digital mengubah administrasi personel tradisional menjadi fungsi pertahanan yang strategis. Digitalisasi proses rekrutmen, penempatan, promosi, hingga pembinaan karier akan memperkuat indeks kesiapan personel dan memastikan distribusi tenaga yang optimal pada operasi gabungan. Sejalan dengan pandangan Singer (2014), manajemen SDM berbasis data tidak hanya meningkatkan efisiensi, tetapi juga memungkinkan penerapan analitik prediktif terhadap kesiapan misi, yang merupakan faktor krusial dalam efektivitas militer abad ke-21.

Selanjutnya, teori *Cyber Security* sebagaimana dikemukakan oleh Richard A. Clarke (2015) memberikan landasan mikro bagi perlindungan infrastruktur informasi pertahanan. Clarke mengidentifikasi tiga prinsip utama dalam keamanan siber, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) atau yang dikenal sebagai *CIA Triad*. Pelanggaran terhadap salah satu prinsip ini dapat menyebabkan kelumpuhan operasional atau paparan strategis yang berbahaya. Dalam konteks TNI, data personel merupakan bagian dari data pertahanan yang bersifat sangat sensitif. Tanpa adanya standar keamanan siber yang baku, TNI menghadapi risiko serius berupa spionase, manipulasi identitas, dan infiltrasi sistem. Bratton (2017) menegaskan bahwa lembaga pertahanan harus menerapkan lapisan keamanan proaktif melalui enkripsi, sistem deteksi intrusi, dan autentikasi akses. Karena itu, integrasi keamanan siber ke dalam sistem informasi personel TNI merupakan kebutuhan teknis sekaligus strategis dalam menjaga integritas operasional organisasi.

Selain keamanan, kemampuan adaptasi organisasi terhadap perubahan teknologi menjadi dimensi penting yang dijelaskan melalui *Dynamic Capability Theory* dari David Teece (1997). Teori ini menyoroti kemampuan institusi untuk berintegrasi,

mengonfigurasi ulang, dan memperbarui kompetensinya secara berkelanjutan dalam menghadapi lingkungan yang dinamis. Dalam konteks militer, hal ini berarti kemampuan belajar adaptif, literasi digital, dan inovasi berkelanjutan di kalangan personel. TNI perlu membangun mekanisme kelembagaan untuk penguatan kapasitas sumber daya manusianya dalam mengoperasikan dan melindungi infrastruktur digital. Eisenhardt dan Martin (2000) menegaskan bahwa *dynamic capabilities* bukanlah kemampuan yang statis, melainkan proses yang terus berubah dan menyesuaikan diri, sebagaimana yang harus dilakukan TNI agar tetap tangkas di tengah percepatan digitalisasi sistem pertahanan.

Dari sisi strategi, teori *Indirect Approach* dari Sir Basil Liddell Hart (1954) menjelaskan bahwa keunggulan militer tidak selalu dicapai melalui konfrontasi langsung, melainkan melalui fleksibilitas, keunggulan informasi, dan kemampuan manuver. Dalam konteks transformasi digital, pendekatan tidak langsung ini diterjemahkan sebagai upaya memanfaatkan teknologi, khususnya sistem berbasis AI, untuk mencapai keunggulan informasi dan adaptabilitas strategis tanpa keterlibatan fisik di medan perang. Dengan demikian, integrasi sistem data personel dapat dipahami sebagai manuver strategis non-kinetik yang bertujuan mencapai dominasi operasional di ranah informasi. Dalam kerangka sosiologis, *Social System Theory* dari Talcott Parsons (1951) memberikan dimensi tambahan melalui model AGIL (Adaptation, Goal Attainment, Integration, Latency). Dalam organisasi militer seperti TNI, sistem informasi berfungsi menjalankan peran integrasi (I) yang menghubungkan unit-unit organisasi dan memastikan kohesi operasional. Digitalisasi meningkatkan adaptasi terhadap ancaman baru (A), memastikan pencapaian tujuan pertahanan (G), memperkuat integrasi antar matra (I), dan memelihara stabilitas budaya serta disiplin institusional (L). Dengan demikian, teori Parsons menjelaskan mengapa kohesi digital memperkuat dimensi struktural sekaligus kultural dari organisasi militer modern.

Selanjutnya, standar keamanan informasi ISO/IEC 27001 (2013) menjadi referensi normatif dalam pengelolaan keamanan data. Standar ini menetapkan sistem manajemen keamanan informasi yang mencakup penilaian risiko, perlindungan data, dan peningkatan berkelanjutan. Penerapan standar ini dalam institusi pertahanan memastikan bahwa aspek kerahasiaan, integritas, dan ketersediaan data dapat diaudit serta dipertanggungjawabkan. Dalam konteks TNI, hal ini berarti seluruh proses pengelolaan data personel—mulai dari rekrutmen hingga penugasan—harus tunduk pada mekanisme kontrol akses, enkripsi data, serta audit keamanan berkala. Standarisasi tersebut mendukung interoperabilitas antar matra sekaligus menyelaraskan kebijakan pertahanan Indonesia dengan norma tata kelola digital global, sebagaimana diadopsi dalam *NATO Information Assurance Policy* (2019).

Untuk memperkuat hubungan antara teori dan praktik, penelitian ini juga memanfaatkan model *Military Effectiveness and Strategic Resource Management (MESDM)* yang dikembangkan oleh Fachrozi (2020). Model ini menjelaskan bahwa efektivitas militer bergantung pada tiga domain yang saling berhubungan: pengembangan kekuatan, integrasi organisasi, dan keselarasan strategis. Dalam konteks TNI, sistem informasi personel digital bukan sekadar alat administratif, tetapi merupakan penggerak utama kesiapan tempur dan keberlanjutan kekuatan pertahanan. Chandler (1962) memperkuat pandangan ini dengan mendefinisikan strategi sebagai penyelarasan jangka panjang antara sumber daya dan tindakan untuk mencapai tujuan organisasi. Sementara itu, *5P Model of Strategy* dari Mintzberg (1994)—yang terdiri atas *Plan, Ploy, Pattern, Position,* dan *Perspective*—memberikan kerangka pemahaman bahwa digitalisasi personel TNI bukan hanya rencana modernisasi teknologis, tetapi juga perubahan struktural menuju fleksibilitas strategis.

Kajian pustaka terdahulu menunjukkan kesadaran global yang meningkat terhadap pentingnya transformasi digital dalam manajemen SDM militer. Peterson (2020) mencatat keberhasilan Angkatan Darat Amerika Serikat dalam menggunakan

sistem HR berbasis *cloud* untuk meningkatkan logistik dan kesiapan, meskipun masih menghadapi kendala interoperabilitas antar matra. Wijaya (2021) menemukan bahwa digitalisasi di TNI AD meningkatkan efisiensi, namun belum sepenuhnya terintegrasi. Hartanto (2022) dan Anderson (2022) menyoroti meningkatnya ancaman siber terhadap basis data militer dan merekomendasikan kerangka keamanan berbasis AI. Prasetyo (2023) menunjukkan peningkatan signifikan dalam efisiensi pengelolaan personel di TNI AU melalui sistem digital, tetapi menegaskan perlunya standardisasi lintas matra. Berdasarkan kesenjangan penelitian tersebut, studi ini menawarkan pendekatan integratif yang belum pernah dilakukan sebelumnya, yaitu perumusan kerangka lintas matra untuk sistem informasi personel TNI yang mampu meningkatkan interoperabilitas, keamanan siber, dan efektivitas operasional secara simultan.

Dengan merujuk pada keseluruhan teori tersebut, fondasi konseptual penelitian ini dibangun atas interaksi tiga dimensi strategis utama: integrasi sistem (System Theory dan MESDM) yang menekankan sinergi operasional melalui arsitektur digital yang interoperabel; adaptasi sumber daya manusia (HRM Theory dan Dynamic Capability) yang menekankan peningkatan kompetensi dan ketangkasan personel dalam ekosistem pertahanan digital; serta keamanan informasi (Cyber Security dan ISO/IEC 27001) yang berfokus pada perlindungan integritas data personel sebagai aset pertahanan utama. Ketiga dimensi teoretis ini secara bersama-sama menjadi dasar dalam perumusan strategi pengembangan sistem informasi personel berbasis teknologi informasi untuk memperkuat kemampuan TNI dalam melaksanakan kampanye militer secara efektif dan aman di era perang berbasis informasi.

3. Metode Penelitian

Penelitian ini menggunakan desain penelitian kualitatif-evaluatif untuk menganalisis pengembangan strategis sistem informasi personel Tentara Nasional Indonesia (TNI) berbasis teknologi informasi (TI). Pendekatan evaluatif dipilih karena

penelitian ini tidak hanya menggambarkan kondisi yang ada, tetapi juga menilai tingkat efektivitas, mengidentifikasi hambatan, serta merumuskan strategi yang dapat diimplementasikan guna memperbaiki sistem yang sedang berjalan. Menurut Creswell (2018), pendekatan evaluatif kualitatif sangat relevan digunakan untuk menganalisis transformasi kelembagaan yang kompleks dan melibatkan dimensi struktural, teknologi, serta sumber daya manusia—kondisi yang sesuai dengan proses transformasi digital yang sedang berlangsung di lingkungan TNI.

Fokus penelitian ini diarahkan pada penilaian terhadap sistem manajemen informasi personel TNI dengan tujuan mengidentifikasi kelemahan dalam aspek infrastruktur, interoperabilitas, dan kapasitas sumber daya manusia. Berdasarkan hasil analisis tersebut, penelitian ini kemudian merumuskan model pengembangan sistem personel digital yang terintegrasi. Kerangka analisis penelitian ini mengombinasikan dua pendekatan utama, yaitu analisis SWOT (*Strengths, Weaknesses, Opportunities, Threats*) dan analisis Fishbone (Ishikawa), yang digunakan untuk menilai faktor internal dan eksternal yang memengaruhi keberhasilan modernisasi sistem informasi personel.

Secara ruang lingkup, penelitian ini ditempatkan pada titik temu antara manajemen pertahanan, sistem informasi, dan pengembangan sumber daya manusia militer. Analisis dilakukan pada tiga lapisan organisasi dalam struktur TNI. Pada tingkat strategis, penelitian berfokus pada Kementerian Pertahanan (Kemhan) dan Markas Besar TNI (Mabes TNI) untuk menelaah kebijakan pertahanan, arah transformasi digital, dan kerangka integrasi data pertahanan. Pada tingkat operasional, penelitian berfokus pada Staf Personel (Spers) Angkatan Darat, Angkatan Laut, dan Angkatan Udara, dengan perhatian utama pada praktik manajemen data, interoperabilitas sistem, serta pelaporan kesiapan personel. Sedangkan pada tingkat taktis, penelitian menelaah satuan pelaksana di lapangan untuk memahami tantangan praktis yang dihadapi dalam proses pembaruan dan sinkronisasi data personel.

Secara temporal, penelitian ini mencakup rentang waktu 2022–2025 yang bertepatan dengan agenda transformasi digital pertahanan nasional sebagaimana diatur dalam *Digital Transformation Roadmap 2025* Kementerian Pertahanan Republik Indonesia.

Data penelitian ini bersumber dari dua jenis data utama, yaitu data primer dan data sekunder. Data primer diperoleh melalui wawancara semi-terstruktur dengan para pejabat dan pakar pertahanan. Informan penelitian mencakup perwira tinggi di Markas Besar TNI (khususnya bidang Binpers dan Pusinfolahta), pejabat Pusat Data dan Informasi Kementerian Pertahanan (Pusdatin Kemhan), instruktur teknologi informasi dari Komando Pendidikan dan Pelatihan TNI (Diklat TNI), serta akademisi Universitas Pertahanan yang memiliki kepakaran dalam bidang teknologi pertahanan dan strategi militer.

Sementara itu, data sekunder diperoleh dari berbagai dokumen resmi pertahanan yang relevan, antara lain: Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara; Undang-Undang Nomor 3 Tahun 2025 tentang Tentara Nasional Indonesia (perubahan atas UU Nomor 34 Tahun 2004); Peraturan Pemerintah Nomor 39 Tahun 2010 tentang Administrasi Personel Militer; Peraturan Menteri Pertahanan Nomor 1 Tahun 2023 tentang *One Defense Data Policy*; serta laporan tahunan Kementerian Pertahanan (Kemhan, 2023) dan laporan tahunan Staf Umum TNI (2022–2023). Seluruh dokumen tersebut memberikan konteks regulatif dan empiris bagi analisis pengembangan sistem informasi personel TNI.

Teknik pengumpulan data dilakukan melalui tiga metode utama. Pertama, wawancara mendalam (*in-depth interview*) dengan sepuluh informan kunci yang mewakili tingkatan strategis, operasional, dan teknis. Wawancara ini diarahkan untuk menggali persepsi dan pengalaman mengenai tantangan integrasi sistem, keamanan data, kompetensi digital personel, dan interoperabilitas antar matra. Seluruh wawancara direkam, ditranskripsi, dan dianalisis secara tematik. Kedua, analisis dokumen dilakukan terhadap laporan kebijakan, hasil audit internal (seperti *Internal*

Audit Report on Personnel Information Systems, Sekjen Kemhan 2023), serta berbagai laporan pertahanan guna mengidentifikasi indikator kinerja kelembagaan, kesenjangan kebijakan, dan inisiatif digital yang sedang berlangsung. Ketiga, triangulasi dilakukan untuk memastikan validitas data, yakni dengan memverifikasi hasil wawancara, dokumen, dan observasi lapangan agar diperoleh konsistensi temuan (Miles, Huberman, & Saldaña, 2014).

Analisis data dilakukan melalui tiga tahap yang bersifat iteratif, yakni reduksi data, penyajian data, dan penarikan kesimpulan. Pada tahap reduksi data, informasi hasil wawancara dan dokumen dikategorikan ke dalam tema-tema utama seperti infrastruktur dan integrasi sistem, kompetensi sumber daya manusia, serta standarisasi keamanan informasi. Pada tahap penyajian data, digunakan alat bantu visual seperti diagram Fishbone untuk memetakan hubungan sebab-akibat dan mengidentifikasi akar permasalahan sistemik, misalnya rendahnya interoperabilitas akibat ketidaksesuaian basis data, keterbatasan tenaga TI, serta fragmentasi kebijakan. Pada tahap terakhir, dilakukan penarikan kesimpulan melalui analisis SWOT dengan temuan utama sebagai berikut: kekuatan berupa dukungan regulasi dan kebijakan transformasi digital (UU No. 3/2025 dan Perpang TNI No. 27/2019); kelemahan berupa fragmentasi sistem informasi dan rendahnya literasi digital; peluang berupa kemajuan pesat dalam teknologi AI, *cloud computing*, dan tata kelola data pertahanan; serta ancaman berupa meningkatnya serangan siber terhadap basis data pertahanan dan keterbatasan tenaga ahli keamanan siber.

Untuk menjamin keandalan metodologis, penelitian ini menerapkan tiga mekanisme validasi. Pertama, *source triangulation* dilakukan dengan memeriksa kesesuaian data antar informan dari institusi berbeda. Kedua, *peer debriefing* dilakukan melalui proses penelaahan hasil analisis oleh dua peneliti pertahanan dari Universitas Pertahanan dan seorang perwira senior Mabes TNI. Ketiga, *audit trail* dilakukan dengan mendokumentasikan seluruh transkrip wawancara, catatan lapangan, dan referensi dokumen secara digital agar dapat ditelusuri dan direplikasi oleh peneliti

lain. Prosedur ini sesuai dengan kriteria reliabilitas penelitian kualitatif sebagaimana dikemukakan oleh Yin (2018), yang menekankan pentingnya kredibilitas dan transferabilitas hasil penelitian.

Mengacu pada sensitivitas data pertahanan dan militer, penelitian ini dijalankan dengan memperhatikan etika penelitian secara ketat. Setiap partisipan diberikan penjelasan mengenai tujuan akademik penelitian dan menyatakan persetujuan (*informed consent*) sebelum wawancara. Seluruh data bersifat anonim untuk menjaga kerahasiaan, dan informasi yang dikategorikan sebagai rahasia negara tidak disertakan dalam publikasi. Penelitian ini mengikuti standar etika penelitian Universitas Pertahanan sebagaimana diatur dalam *Kode Etik Penelitian Pertahanan 2024*.

Secara keseluruhan, kerangka metodologis ini memungkinkan evaluasi komprehensif terhadap sistem informasi personel TNI dengan memadukan dimensi empiris, regulatif, dan strategis. Kombinasi antara analisis SWOT dan Fishbone memberikan dasar yang kuat untuk mengidentifikasi akar penyebab permasalahan serta merancang intervensi strategis yang realistis guna meningkatkan interoperabilitas sistem, kompetensi sumber daya manusia, dan ketahanan siber dalam mendukung modernisasi pertahanan nasional.

4. Hasil Penelitian dan Analisis

Analisis kualitatif-evaluatif menunjukkan bahwa Tentara Nasional Indonesia (TNI) telah mengalami kemajuan yang terukur dalam upaya digitalisasi sistem manajemen personel. Namun demikian, kemajuan tersebut masih dibatasi oleh sejumlah persoalan struktural yang signifikan, terutama pada aspek integrasi infrastruktur, kompetensi sumber daya manusia, dan standarisasi sistem informasi. Temuan empiris menunjukkan bahwa baru sekitar 65% sistem informasi personel TNI yang terintegrasi dengan platform digital, sementara 35% satuan masih bergantung pada prosedur manual (Kementerian Pertahanan RI, 2023). Ketidakseimbangan ini

mengakibatkan keterlambatan sinkronisasi data, ketidakkonsistenan data personel, serta inefisiensi fungsi komando dan pengendalian (*Command and Control* / C2) dalam operasi gabungan. Lebih jauh lagi, sekitar 60% personel belum memperoleh pelatihan teknologi informasi yang memadai (Diklat TNI, 2023), sehingga adopsi prosedur digital baru berjalan lambat. Tidak adanya standar data yang seragam antar matra juga berdampak serius bagi interoperabilitas; hanya sekitar 55% data personel yang dapat diakses secara lintas Angkatan Darat, Angkatan Laut, dan Angkatan Udara (Spers Mabes TNI, 2022). Dengan demikian, terdapat tiga masalah inti yang menjadi fokus kajian ini, yaitu keterbatasan infrastruktur digital dan rendahnya tingkat integrasi sistem, keterbatasan kompetensi digital personel militer, serta belum adanya tata kelola terpadu terkait data dan keamanan siber. Ketiga persoalan ini selanjutnya dibahas secara mendalam beserta implikasinya terhadap efektivitas militer dan agenda modernisasi pertahanan nasional.

Dari sisi infrastruktur dan integrasi sistem, pengembangan infrastruktur digital TNI masih belum merata di antara ketiga matra. TNI Angkatan Darat relatif lebih maju melalui program uji coba *Human Resource Information System* (HRIS) internal, sementara TNI Angkatan Laut dan TNI Angkatan Udara masih banyak bergantung pada basis data terpisah yang dikelola oleh masing-masing staf personel. Dalam konteks operasi lapangan—misalnya pada operasi pengamanan di Papua dan pengamanan perbatasan Kalimantan—pertukaran data personel antar komando kerap mengalami keterlambatan dan ketidakcocokan format akibat perbedaan sistem jaringan dan struktur data. Ketidaktersediaan platform yang benar-benar interoperabel menyebabkan Komando Gabungan Wilayah Pertahanan (Kogabwilhan) tidak selalu dapat mengakses data personel secara terpadu dan real time. Kondisi ini melemahkan kesiapsiagaan serta kemampuan pengerahan cepat (*rapid deployment capability*), dua elemen yang menjadi syarat keberhasilan kampanye militer modern (Gray, 2010). Analisis Fishbone mengungkap bahwa akar masalahnya meliputi fragmentasi kebijakan, karena tiap matra mempertahankan kemandirian arsitektur

datanya sendiri tanpa ada otoritas pusat yang berfungsi memaksa integrasi; disparitas teknologi, berupa perbedaan perangkat keras dan perangkat lunak yang diadakan secara sektoral sehingga tidak kompatibel; serta kesenjangan prioritas anggaran, yaitu investasi infrastruktur digital yang masih dianggap sekunder dibanding modernisasi kemampuan kinetik seperti alutsista dan dukungan logistik. Temuan ini konsisten dengan hasil studi Peterson (2020) dan Wijaya (2021) yang menekankan bahwa kegagalan interoperabilitas dalam sistem pertahanan digital lebih sering disebabkan oleh segmentasi birokratis daripada sekadar persoalan teknis. Dari perspektif manajemen strategis, ketidakselarasan sistem ini menurunkan efisiensi C2 dan *situational awareness*, dua indikator kunci keberhasilan operasi dalam era digital. Merujuk pada *System Theory* (Ackoff, 1974), ketiadaan sinergi antar subsistem akan berujung pada inefisiensi sistemik; oleh karena itu, integrasi bukan hanya kebutuhan teknis, melainkan kebutuhan organisasional. Untuk itu, penelitian ini merekomendasikan pembentukan suatu lembaga integratif bernama *Defense Digital Integration Center* (DDIC) di bawah Kementerian Pertahanan, yang bertugas menjamin interoperabilitas seluruh basis data personel TNI melalui infrastruktur berbasis *cloud* dan penggunaan protokol *Application Programming Interface* (API) yang memungkinkan sinkronisasi data lintas matra secara standar.

Dimensi kedua berkaitan dengan kompetensi sumber daya manusia dalam proses digitalisasi. Aspek manusia terbukti menjadi faktor paling krusial dalam keberhasilan transformasi digital pertahanan. Meskipun terdapat arah kebijakan modernisasi, tingkat literasi digital di kalangan personel TNI secara umum masih terbatas. Data Komando Pendidikan dan Pelatihan TNI (Diklat TNI, 2023) menunjukkan bahwa hanya sekitar 40% perwira dan bintara yang telah memperoleh pelatihan formal terkait pengelolaan data digital, keamanan siber, atau pemanfaatan sistem pendukung keputusan berbasis AI. Ketiadaan kerangka pengembangan profesional berkelanjutan memperburuk situasi ini. Banyak personel mengalami rotasi jabatan secara periodik tanpa adanya mekanisme retensi kompetensi digital,

sehingga kesenjangan keahlian terus berulang. Analisis SWOT yang diterapkan dalam penelitian ini mengidentifikasi bahwa TNI sebenarnya memiliki kekuatan berupa infrastruktur kelembagaan pendidikan militer seperti Universitas Pertahanan (Unhan RI) dan Sekolah Staf dan Komando (Sesko TNI), yang secara potensial mampu merancang kurikulum pertahanan digital berbasis kebutuhan operasional. Namun kelemahannya adalah belum adanya standardisasi sertifikasi keterampilan digital dan ketidakseragaman pola pelatihan antar matra. Peluangnya adalah tersedianya tren global dan jejaring kerja sama pendidikan pertahanan berbasis digital, sementara ancaman utamanya adalah meningkatnya insiden serangan siber yang secara khusus menargetkan sistem sumber daya manusia militer (Hartanto, 2022; Anderson, 2022).

Berdasarkan temuan tersebut, penelitian ini mengusulkan sebuah model pengembangan yang berfokus pada peningkatan kapasitas digital personel, yang dirumuskan sebagai *Digital Competence Enhancement Model* (DCEM). Model ini dibangun di atas teori manajemen sumber daya manusia (Ulrich, 1997; Armstrong, 2014) dan teori *Dynamic Capability* (Teece, 1997), dan terdiri dari tiga pilar utama. Pilar pertama adalah pembelajaran institusional, yakni integrasi mata kuliah dan modul pertahanan digital secara sistematis dalam kurikulum pendidikan militer reguler. Pilar kedua adalah sertifikasi kompetensi, yaitu penerapan skema sertifikasi teknologi informasi dan keamanan siber yang dirancang khusus untuk kebutuhan pertahanan dan disejajarkan dengan standar ISO/IEC 27001. Pilar ketiga adalah retensi talenta, yakni pembentukan semacam *Defense Digital Reserve Corps* sebagai mekanisme menjaga kesinambungan personel yang memiliki kompetensi digital tinggi agar tidak hilang saat terjadi rotasi jabatan maupun penugasan operasi. Strategi yang berpusat pada manusia ini selaras dengan kerangka AGIL (Parsons, 1951), di mana fungsi adaptasi (A) dan integrasi (I) organisasi dipertahankan melalui pembelajaran kelembagaan dan penguatan kapabilitas individu. Peningkatan kompetensi digital personel secara langsung berdampak pada ketangkasan operasional TNI: kecepatan input dan validasi data meningkat, pemetaan personel menjadi lebih akurat, dan

siklus pengambilan keputusan menjadi lebih singkat. Pada saat yang sama, literasi digital yang lebih tinggi memperkuat kesiapsiagaan siber dengan menurunkan kerentanan akibat kesalahan manusia, yang secara global diperkirakan berkontribusi terhadap hampir 60% pelanggaran keamanan data di institusi militer (Clarke, 2015). Dengan demikian, pengembangan kapasitas manusia harus ditempatkan sebagai *force multiplier* utama dalam agenda transformasi digital TNI.

Dimensi ketiga terkait dengan standarisasi dan keamanan informasi. Meskipun Kementerian Pertahanan telah menerbitkan Peraturan Menteri Pertahanan Nomor 1 Tahun 2023 tentang Satu Data Pertahanan (*One Defense Data Policy*), implementasi tata kelola data yang benar-benar terpadu di lingkungan TNI masih belum optimal. Setiap matra masih menjalankan protokol enkripsi dan mekanisme pengendalian akses yang berbeda-beda, sehingga menghasilkan kerangka keamanan siber yang terfragmentasi. Audit internal Sekretariat Jenderal Kementerian Pertahanan pada tahun 2023 menunjukkan bahwa meskipun sekitar 65% basis data personel telah terdigitalisasi, kurang dari setengahnya memenuhi tolok ukur kepatuhan ISO/IEC 27001 terkait integritas dan kerahasiaan data. Penelitian ini mengidentifikasi tiga kelemahan utama yang saling berkaitan: pertama, ketiadaan komando keamanan siber terpusat. Pusat Informasi dan Pengolahan Data (Pusinfolahta) TNI hingga kini berfungsi terutama sebagai unit teknis operasional TI, belum memiliki kewenangan regulatif untuk memaksakan protokol keamanan terpadu lintas matra. Kedua, terbatasnya pelatihan ketahanan siber bagi petugas administrasi personel; banyak operator sistem belum memiliki kemampuan untuk mendeteksi atau merespons ancaman seperti phishing, malware, atau ancaman dari orang dalam (*insider threat*). Ketiga, belum adanya mekanisme audit yang seragam dan berkelanjutan untuk memastikan kepatuhan terhadap kebijakan keamanan siber pertahanan secara menyeluruh.

Untuk menjawab kerentanan tersebut, penelitian ini mengajukan rancangan *Standardized Information Security Framework* (SISF) bagi TNI. Rancangan ini mencakup tiga komponen utama. Pertama, penerapan protokol klasifikasi data yang seragam

dengan kategori tingkat sensitivitas (misalnya: Terbatas, Rahasia, Sangat Rahasia) guna mengatur tingkat perlindungan dan akses. Kedua, penerapan sistem pemantauan berbantuan AI yang mampu melakukan deteksi intrusi secara otomatis, mengidentifikasi anomali perilaku akses data, serta menghasilkan pelaporan dini atas potensi pelanggaran. Ketiga, penyusunan peta jalan sertifikasi ISO/IEC 27001 secara bertahap yang mewajibkan seluruh sistem manajemen personel memperoleh status kepatuhan keamanan informasi dalam jangka waktu tertentu. Rekomendasi ini sejalan dengan praktik terbaik lembaga pertahanan Barat, seperti NATO, dan konsisten dengan prinsip-prinsip *Cyber Security Theory* (Clarke, 2015) yang menempatkan kerahasiaan, integritas, dan ketersediaan (CIA) sebagai fondasi sistem informasi pertahanan. Selain itu, aspek etis juga harus dipertimbangkan secara serius. Integrasi kecerdasan buatan dalam sistem personel menimbulkan persoalan akuntabilitas dan transparansi pengambilan keputusan. Literatur etika pertahanan mutakhir menegaskan bahwa penerapan AI dalam domain militer harus tunduk pada prinsip tanggung jawab, transparansi, dan integritas data; dengan kata lain, rekomendasi berbasis AI tetap harus berada di bawah pengawasan dan pertanggungjawaban pengambil keputusan manusia. Dari sudut pandang strategis, standarisasi sistem informasi tidak hanya meningkatkan efisiensi komando, tetapi juga memperkuat posisi diplomasi pertahanan Indonesia. Interoperabilitas dengan negara sahabat—khususnya dalam kerangka kerja sama pertahanan kawasan ASEAN—menuntut kesesuaian dengan norma keamanan data internasional. Dengan demikian, standardisasi berfungsi bukan hanya sebagai mekanisme efisiensi internal, tetapi juga sebagai instrumen kebijakan pertahanan luar negeri.

Berdasarkan keseluruhan temuan tersebut, penelitian ini merumuskan suatu model strategis terintegrasi yang disebut *Integrated Personnel Information Strategy* (IPIS) untuk TNI. Model ini disusun di atas landasan *System Theory*, teori Manajemen Sumber Daya Manusia (HRM), dan standar Keamanan Siber. IPIS mencakup tiga komponen utama. Pertama, integrasi kecerdasan buatan (AI), yang mencakup

penggunaan analitik prediktif untuk memproyeksikan kesiapan personel dan mengoptimalkan rotasi penugasan, serta pemanfaatan algoritma *machine learning* untuk mendeteksi anomali dalam rekam data personel dan kinerja. Kedua, analitik *Big Data*, yakni penggabungan data lintas matra ke dalam dasbor terpadu yang dapat diakses oleh pimpinan komando untuk mendukung pengambilan keputusan terkait distribusi kekuatan manusia secara cepat dalam suatu kampanye militer. Ketiga, infrastruktur komputasi awan (*cloud computing*), berupa penyimpanan data terpusat yang memungkinkan akses aman dan terukur bagi seluruh matra, termasuk penerapan arsitektur *hybrid cloud* (kombinasi *private cloud* dan *public cloud*) untuk menyeimbangkan antara kebutuhan keamanan dan fleksibilitas operasional. Model ini dirancang untuk diimplementasikan secara bertahap: tahap jangka pendek (2025–2026) berfokus pada pembentukan DDIC dan uji coba integrasi di Kogabwilhan I; tahap jangka menengah (2027–2028) memperluas integrasi ke seluruh matra beserta modul AI dan keamanan siber yang terstandar; dan tahap jangka panjang (2029–2030) menargetkan pelembagaan sistem "Satu Data Personel Pertahanan" yang telah tersertifikasi ISO dan selaras dengan kebijakan transformasi digital pertahanan nasional. Secara proyeksi, model ini diharapkan mampu meningkatkan efisiensi operasional melalui percepatan sekitar 40% dalam proses verifikasi data dan pengerahan personel, meningkatkan akurasi fungsi C2 melalui pemantauan kesiapan kekuatan manusia secara waktu nyata, serta memperkuat ketahanan siber dengan meminimalkan kerawanan sistemik lintas matra. Kerangka ini konsisten dengan model *Military Effectiveness and Strategic Resource Management* (MESDM) yang dikembangkan oleh Fachrozi (2020), yang menautkan kapabilitas teknologi, manajemen sumber daya manusia, dan keselarasan strategis sebagai tiga pilar utama efektivitas pertahanan.

Secara strategis, penerapan kerangka ini akan memperkuat transformasi pertahanan Indonesia pada sedikitnya empat dimensi kunci. Pertama, kesiapan komando: sistem terintegrasi memungkinkan pengambil keputusan mengakses data

personel yang akurat secara segera. Kedua, fleksibilitas operasional: basis data yang interoperabel memungkinkan pengerahan kekuatan yang adaptif dalam operasi gabungan maupun dalam konteks peperangan hibrida. Ketiga, ketahanan siber: protokol keamanan siber yang terstandar akan menurunkan kerentanan terhadap spionase digital dan sabotase informasi. Keempat, diplomasi pertahanan: kepatuhan pada standar data internasional meningkatkan kemampuan interoperabilitas dengan negara mitra dan memperkuat posisi Indonesia dalam jejaring keamanan kawasan. Dari sudut pandang teoretis, temuan penelitian ini mengukuhkan beberapa argumen pokok. Pertama, *System Theory* (Bertalanffy; Ackoff) kembali menegaskan bahwa sinergi antar subsistem merupakan prasyarat efisiensi pertahanan. Kedua, teori *Dynamic Capability* (Teece) tervalidasi melalui bukti bahwa pembelajaran adaptif dan pembaruan kompetensi personel merupakan syarat mutlak bagi transformasi pertahanan digital. Ketiga, *Cyber Security Theory* (Clarke) menunjukkan bahwa faktor manusia merupakan pusat dari ketahanan sistem, karena integritas dan reliabilitas data pertahanan pada akhirnya tetap bertumpu pada operator manusia yang terlatih. Secara keseluruhan, temuan ini memperluas kerangka pemikiran tentang *Digital Defense Governance*, yakni pandangan bahwa institusi pertahanan harus dipahami sebagai sistem sosio-teknis, di mana teknologi, modal manusia, dan integrasi organisasi harus berkembang secara simultan.

Dengan demikian dapat dipahami modernisasi sistem informasi personel TNI bukan sekadar proyek teknologi, melainkan transformasi strategis yang mencakup reformasi organisasi, peningkatan literasi digital, dan pembangunan ketahanan siber. Implementasi sistem personel berbasis TI yang terintegrasi akan memperkuat sinkronisasi C2, mengoptimalkan manajemen kekuatan manusia, dan meningkatkan daya tangkal strategis Indonesia dalam ruang tempur digital. Hasil ini menempatkan TNI sebagai institusi pertahanan yang adaptif secara teknologi, berbasis data, dan mampu mempertahankan keunggulan operasional di tengah kompleksitas lanskap peperangan abad ke-21.

5. Kesimpulan

Temuan penelitian ini menegaskan bahwa modernisasi sistem informasi personel Tentara Nasional Indonesia (TNI) merupakan kebutuhan strategis bagi penguatan kesiapsiagaan pertahanan nasional pada era digital. Kondisi saat ini, yang ditandai oleh integrasi digital yang masih parsial (sekitar 65%), ketimpangan infrastruktur teknologi informasi, serta keterbatasan interoperabilitas antar matra, menunjukkan bahwa transformasi digital dalam manajemen personel pertahanan masih berada pada fase transisional. Sepanjang penelitian ini diidentifikasi tiga tantangan utama. Pertama, keterbatasan infrastruktur digital dan ketiadaan interoperabilitas yang optimal antara Angkatan Darat, Angkatan Laut, dan Angkatan Udara. Kedua, rendahnya tingkat kompetensi digital dan literasi teknologi di kalangan personel, yang membatasi utilisasi dan pemeliharaan sistem digital. Ketiga, belum adanya kerangka baku keamanan informasi, yang berdampak pada kerentanan kebocoran data serta inefisiensi fungsi komando dan pengendalian (*Command and Control* / C2).

Dengan menggunakan kerangka *System Theory* (Bertalanffy, 1968), penelitian ini menyimpulkan bahwa manajemen personel dalam TNI harus diposisikan sebagai subsistem inti dari arsitektur pertahanan yang lebih luas. Hubungan saling ketergantungan antara subsistem sumber daya manusia, operasi, logistik, dan intelijen hanya dapat berfungsi efektif apabila ditopang oleh platform digital terintegrasi. Selain itu, hasil penelitian ini juga menegaskan kembali tesis Teece (1997) dalam *Dynamic Capability Theory*, yakni bahwa keberhasilan organisasi dalam melakukan transformasi digital sangat ditentukan oleh kapasitas adaptif, pembelajaran berkelanjutan, dan pembaruan teknologi pada level sumber daya manusia. Lebih jauh, adopsi prinsip keamanan siber yang selaras dengan standar ISO/IEC 27001 diperlukan agar transformasi digital pertahanan berjalan seiring dengan standar global terkait kerahasiaan, integritas, dan ketersediaan data (CIA Triad). Integrasi kecerdasan buatan (Artificial Intelligence/AI), analitik *Big Data*, dan

cloud computing dalam sistem informasi personel diproyeksikan akan meningkatkan akurasi pengambilan keputusan berbasis data, mempercepat proses pengerahan personel, serta memperkuat ketahanan nasional terhadap ancaman perang hibrida dan siber. Dengan demikian, transformasi digital manajemen personel TNI tidak sekadar merupakan pembaruan teknologi administratif, melainkan suatu reformasi sistemik—evolusi kelembagaan menuju apa yang disebut Gray (2010) sebagai *strategic coherence*, yaitu keterpaduan antara sarana, metode, dan tujuan untuk memastikan kapabilitas militer yang efektif.

Rekomendasi

Berdasarkan analisis di atas, penelitian ini mengajukan sejumlah rekomendasi strategis dan kebijakan untuk memandu Kementerian Pertahanan dan Markas Besar TNI dalam mempercepat digitalisasi pertahanan. Pertama, diperlukan pembentukan suatu struktur komando khusus di bawah Kementerian Pertahanan yang berfungsi mengoordinasikan integrasi sistem digital di seluruh matra, yaitu *Defense Digital Integration Command* (DDIC). Komando ini bertugas melakukan standarisasi platform TI, menegakkan protokol interoperabilitas, serta mengelola basis data personel terpusat berbasis infrastruktur *cloud* dengan model akses hibrida yang aman dan terukur. Kedua, diperlukan program penguatan kompetensi digital personel TNI secara sistematis. Sistem pendidikan TNI, mulai dari pendidikan dasar hingga sekolah staf dan komando, perlu memasukkan modul literasi digital dan keamanan siber sebagai muatan wajib. Hal ini sejalan dengan *Digital Competence Enhancement Model* (DCEM) yang diajukan dalam penelitian ini, yang menitikberatkan pada pembelajaran institusional, sertifikasi kompetensi, serta retensi talenta digital pertahanan. Kolaborasi terstruktur dengan lembaga akademik seperti Universitas Pertahanan dan lembaga teknologi pertahanan nasional akan mempercepat pembentukan kapasitas tersebut. Ketiga, perlu dilakukan pembaruan kerangka hukum dan regulasi. Peraturan perundang-undangan yang saat ini mengatur

administrasi personel militer—khususnya Peraturan Pemerintah Nomor 39 Tahun 2010—perlu direvisi agar mencakup tata kelola keamanan siber, perlindungan data personel militer, serta prinsip etika kecerdasan buatan. Penguatan aspek regulatif ini penting untuk membangun akuntabilitas digital kelembagaan dan memperjelas otoritas serta tanggung jawab antara Kementerian Pertahanan dan TNI dalam pengelolaan data pertahanan. Keempat, dari aspek implementasi teknologi, TNI perlu mengadopsi sistem analitik personel berbasis AI yang mampu memproyeksikan tingkat kesiapan, mengoptimalkan rotasi, dan mengotomatiskan alur kerja administratif. Jika dikombinasikan dengan analitik *Big Data* dan platform *cloud computing*, integrasi ini akan menghasilkan visualisasi kesiapan personel secara waktu nyata bagi seluruh tingkat komando, yang pada gilirannya akan meningkatkan akurasi pengambilan keputusan dan efektivitas C2. Kelima, dari perspektif keamanan siber, perlu disusun peta jalan sertifikasi ISO/IEC 27001 yang dilaksanakan secara bertahap dan menargetkan kepatuhan penuh seluruh sistem informasi personel TNI paling lambat tahun 2030. Peta jalan ini harus mencakup audit keamanan rutin, uji penetrasi (*penetration testing*), serta pemantauan berkelanjutan melalui sistem deteksi intrusi berbantuan AI. Inisiatif ini bukan hanya meningkatkan resiliensi siber pertahanan nasional, tetapi juga menyelaraskan praktik pengelolaan data pertahanan Indonesia dengan tolok ukur keamanan siber internasional.

Implementasi kerangka strategis di atas diproyeksikan akan menghasilkan empat dampak jangka panjang terhadap postur pertahanan Indonesia.

Pertama, peningkatan efisiensi operasional melalui sinkronisasi data dan pengerahan personel yang lebih cepat dalam operasi gabungan.

Kedua, peningkatan kelincahan komando, karena koordinasi C2 akan ditopang oleh akses real-time terhadap basis data personel yang terpadu.

Ketiga, peningkatan ketahanan siber melalui standar keamanan yang seragam, yang berdampak pada penurunan kerentanan terhadap serangan siber, sabotase data, dan spionase digital, sekaligus memperkuat integritas data pertahanan.

Keempat, penguatan posisi kepemimpinan regional Indonesia dalam tata kelola pertahanan digital, khususnya di kawasan Asia Tenggara, melalui peningkatan interoperabilitas dengan sistem pertahanan negara-negara ASEAN maupun mitra strategis lainnya.

Dalam perspektif strategis, keberhasilan transformasi ini akan sangat menentukan kemampuan TNI untuk beradaptasi dengan karakter peperangan hibrida abad ke-21, di mana kecepatan data dan integritas digital menjadi sama pentingnya dengan daya gempur kinetik. Sejalan dengan penegasan Gray (2010) bahwa revolusi sejati dalam urusan militer tidak terletak semata pada senjata, melainkan pada informasi, prinsip tersebut menangkap esensi dari agenda transformasi ini: membangun organisasi militer yang cerdas, adaptif, dan berdaulat secara digital.

Daftar Pustaka

Ackoff, R. L. (1974). *Redesigning the Future: A Systems Approach to Societal Problems.* New York: John Wiley & Sons.

Anderson, R. (2022). *Cybersecurity in Military Human Resource Systems: Risks and Policy Responses. Defense Technology Review, 18*(3), 115–128. https://doi.org/10.1080/deftech.2022.1153

Armstrong, M. (2014). *Armstrong's Handbook of Human Resource Management Practice* (13th ed.). London: Kogan Page.

Bertalanffy, L. von. (1968). *General System Theory: Foundations, Development, Applications.* New York: George Braziller.

Bratton, J. (2017). *Work and Organizational Behaviour* (3rd ed.). London: Palgrave Macmillan.

Chandler, A. D. (1962). *Strategy and Structure: Chapters in the History of the Industrial Enterprise.* Cambridge, MA: MIT Press.

Checkland, P. (1981). *Systems Thinking, Systems Practice.* Chichester: John Wiley & Sons.

Clarke, R. A. (2015). *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Ecco Press.

Creswell, J. W. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). Thousand Oaks, CA: SAGE Publications.

Dessler, G. (2019). *Human Resource Management* (16th ed.). Boston: Pearson Education.

Eisenhardt, K. M., & Martin, J. A. (2000). *Dynamic Capabilities: What Are They? Strategic Management Journal, 21*(10–11), 1105–1121. https://doi.org/10.1002/1097-0266(200010/11)

Fachrozi, M. (2020). *Military Effectiveness and Strategic Resource Management (MESDM): A Framework for Defense Human Capital. Jurnal Pertahanan dan Bela Negara, 10*(2), 145–167.

Gharajedaghi, J. (2011). *Systems Thinking: Managing Chaos and Complexity* (3rd ed.). Burlington, MA: Elsevier.

Gray, C. S. (1999). *Modern Strategy.* Oxford: Oxford University Press.

Gray, C. S. (2010). *The Strategy Bridge: Theory for Practice.* Oxford: Oxford University Press.

Hartanto, A. (2022). *Digital Transformation and Cybersecurity in the Indonesian Armed Forces. Jurnal Teknologi Pertahanan, 8*(1), 51–74.

International Organization for Standardization (ISO). (2013). *ISO/IEC 27001:2013 – Information Security Management Systems — Requirements.* Geneva: ISO.

Kemhan RI. (2023). *Laporan Tahunan Transformasi Digital Pertahanan 2023.* Jakarta: Kementerian Pertahanan Republik Indonesia.

Liddell Hart, B. H. (1954). *Strategy: The Indirect Approach.* London: Faber and Faber.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (3rd ed.). Thousand Oaks, CA: SAGE Publications.

Mintzberg, H. (1994). *The Rise and Fall of Strategic Planning.* New York: Free Press.

Nugroho, D. (2023). *Threat Perception and Digital Defense Readiness in Indonesia. Journal of Strategic Studies, 25*(2), 98–116.

Parsons, T. (1951). *The Social System.* Glencoe, IL: Free Press.

Peterson, M. (2020). *Cloud-Based HR Systems in the U.S. Army: Lessons for Defense Digitalization. Defense Information Review, 12*(4), 201–222.

Prasetyo, B. (2023). *Evaluating the Digital Personnel System in the Indonesian Air Force. Jurnal Kebijakan Pertahanan, 9*(3), 45–67.

Singer, P. W. (2014). *Wired for War: The Robotics Revolution and Conflict in the 21st Century.* New York: Penguin Press.

Stanford Encyclopedia of Philosophy. (2023). *Ethics of Artificial Intelligence and Military Applications.* Stanford University. Retrieved from https://plato.stanford.edu/entries/ethics-ai-military/

Teece, D. J. (1997). *Dynamic Capabilities and Strategic Management. Strategic Management Journal, 18*(7), 509–533. https://doi.org/10.1002/(SICI)1097-0266

Ulrich, D. (1997). *Human Resource Champions: The Next Agenda for Adding Value and Delivering Results.* Boston: Harvard Business School Press.

Walt, S. M. (1987). *The Origins of Alliances.* Ithaca, NY: Cornell University Press.

Wijaya, R. (2021). *Interoperability Challenges in the Digital Transformation of the Indonesian Army. Jurnal Ilmu Pertahanan, 7*(2), 80–103.

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). Thousand Oaks, CA: SAGE Publications.