PERAN SISTEM INFORMASI DAN DEFEND ID DALAM PENGUATAN PERTAHANAN NASIONAL ERA DIGITAL

Syariefa Alya, IB Putra Jandhana, Gregorius Henu Basworo
Industri Pertahanan, Universitas Pertahanan Republik Indonesia
Kawasan IPSC Sentul, Sukahati, Kec. Citeureup, Kabupaten Bogor, Jawa Barat 16810
syariefa.alya@tp.idu.ac.id

ABSTRAK

Transformasi digital dalam industri pertahanan menjadi krusial di tengah meningkatnya ancaman siber terhadap sistem informasi strategis nasional. Kasus peretasan situs Kementerian Pertahanan menjadi indikasi lemahnya ketahanan siber nasional. DEFEND ID sebagai holding BUMN industri pertahanan memiliki peran strategis dalam mengintegrasikan sistem informasi guna memperkuat pertahanan negara. Namun, permasalahan seperti ketergantungan terhadap teknologi asing, keterbatasan sumber daya manusia, dan ketiadaan standar interoperabilitas masih menjadi tantangan signifikan. Penelitian ini bertujuan untuk mengkaji peran sistem informasi dan strategi DEFEND ID dalam mendukung ketahanan pertahanan nasional era digital. Metode yang digunakan adalah deskriptif kualitatif berbasis studi pustaka, dengan pendekatan tematik dan analisis SWOT. Hasil penelitian menunjukkan bahwa penerapan sistem ERP dan MES di lingkungan DEFEND ID telah meningkatkan efisiensi produksi dan distribusi logistik. Pengujian menunjukkan peningkatan efisiensi distribusi logistik sebesar 17%, dan penurunan biaya operasional sebesar 12%. Namun demikian, integrasi sistem nasional masih terhambat oleh fragmentasi teknologi dan lemahnya koordinasi antar entitas pertahanan. Penelitian ini merekomendasikan pembentukan pusat data militer nasional, pengembangan sistem informasi mandiri, serta penguatan kolaborasi triple helix. Temuan ini menegaskan urgensi reformasi sistem informasi pertahanan sebagai fondasi kemandirian teknologi nasional.

Kata kunci : *Sistem Informasi, DEFEND ID, Pertahanan Nasional, Transformasi Digital, Keamanan Siber, Interoperabilitas.*

1. PENDAHULUAN

Dalam beberapa tahun terakhir, diskursus mengenai penguatan pertahanan negara tidak lagi berkutat hanya pada peningkatan jumlah personel militer atau modernisasi alat utama sistem persenjataan (alutsista), tetapi semakin mengarah pada pentingnya transformasi digital di sektor pertahanan. Dunia saat ini tengah menyaksikan bagaimana ancaman terhadap suatu negara tak selalu datang dari medan tempur, melainkan juga melalui serangan di ruang siber—tanpa suara tembakan, tapi mampu melumpuhkan sistem kendali pertahanan dan mengekstrak data strategis dalam hitungan menit. Indonesia bukan pengecualian. Insiden kebocoran data pada situs Kementerian Pertahanan RI tahun 2023 menjadi contoh nyata yang menyadarkan berbagai pihak bahwa ancaman terhadap keamanan nasional kini juga berasal dari ranah digital [1].

Sayangnya, sistem informasi pertahanan Indonesia saat ini masih berada dalam kondisi yang belum sepenuhnya siap. Berbagai BUMN strategis di bawah naungan DEFEND ID seperti PT Pindad, PT Dahana, PT PAL, PT LEN, dan PT Dirgantara Indonesia masih menggunakan sistem yang berdiri sendiri, tidak terintegrasi, dan memiliki standar keamanan yang berbeda-beda. Hal ini menimbulkan banyak konsekuensi, mulai dari inkonsistensi data logistik militer, keterlambatan dalam koordinasi, hingga potensi kerentanan terhadap serangan siber yang menyasar titik-titik lemah dalam sistem yang tidak sinkron [2]. Sebuah sistem pertahanan yang ideal mestinya dibangun di atas sistem informasi yang tidak hanya kuat secara teknologi, tetapi juga mampu menyatukan seluruh entitas strategis di bawah satu ekosistem digital yang saling terhubung dan saling mengamankan.

Mengacu pada definisi yang dikemukakan oleh Priyono (2024), transformasi digital dalam industri pertahanan menjadi krusial di tengah meningkatnya ancaman siber terhadap sistem informasi strategis nasional. [3]. Dalam kerangka pertahanan nasional, sistem informasi menjadi landasan utama dari berbagai fungsi strategis mulai dari perencanaan logistik militer, pemantauan alutsista, hingga komunikasi komando dan kendali. Artinya, tanpa sistem informasi yang kokoh dan aman, keberlangsungan operasi pertahanan bisa terganggu, dan dalam konteks tertentu, bisa membahayakan kedaulatan negara.

Yang lebih mengkhawatirkan, hingga kini Indonesia belum memiliki pusat data pertahanan nasional yang berdiri secara independen dan terlindungi oleh sistem enkripsi buatan dalam negeri. Padahal, Pemerintah Indonesia melalui Kementerian Pertahanan Republik Indonesia (2025) terus membangun ketangguhan cybersecurity sebagai bagian dari strategi penguatan sistem pertahanan digital dalam menghadapi ancaman siber yang terus berkembang. [4]. Namun, dalam praktiknya, sistem informasi yang digunakan di sektor pertahanan sebagian besar masih bergantung pada vendor asing, termasuk dalam hal platform software, sistem ERP, dan bahkan sistem komunikasi data. Ketergantungan

ini tidak hanya menciptakan kerentanan keamanan, tetapi juga menutup ruang inovasi teknologi dalam negeri.

Beberapa perusahaan dalam DEFEND ID memang telah memulai langkah ke arah digitalisasi. Sebagai contoh, PT Dahana telah mengimplementasikan sistem ERP dan MES untuk mendukung proses produksi bahan peledak secara lebih efisien dan terukur [5]. Namun, keberhasilan internal semacam ini tidak akan berdampak signifikan apabila tidak ditopang oleh kebijakan terintegrasi lintas entitas. Seperti yang dijelaskan oleh David, sistem informasi strategis hanya dapat menghasilkan keunggulan kompetitif bila dibangun berdasarkan kerangka strategi perusahaan yang solid dan dipadukan dengan pengelolaan perubahan yang terstruktur [6].

Dalam konteks pertahanan, keberhasilan transformasi digital bukan hanya soal efisiensi, tetapi juga tentang keamanan, integrasi, dan kecepatan respons terhadap situasi kritis. Sutomo et al. (2025) menekankan pentingnya pengembangan strategi pertahanan digital yang berbasis pada manajemen risiko yang baik dan kolaborasi lintas sektor dalam meningkatkan ketahanan siber di sektor pertahanan. [7]. Bagi Indonesia, ini berarti pembangunan sistem informasi pertahanan tidak bisa lagi dilakukan secara parsial atau sektoral, melainkan harus dikelola sebagai proyek strategis nasional yang melibatkan koordinasi lintas sektor.

Namun, tantangan besar lainnya terletak pada sumber daya manusia. Laporan dari BSSN menunjukkan bahwa sebagian besar personel yang menangani sistem informasi di sektor pertahanan belum memiliki kompetensi yang memadai dalam bidang keamanan siber. Dari total SDM yang tersedia, hanya sekitar 21% yang memiliki sertifikasi teknis atau pelatihan formal dalam penanganan ancaman siber [8]. Ini menjadi masalah serius, mengingat serangan digital terhadap infrastruktur pertahanan tidak hanya semakin sering terjadi, tetapi juga semakin kompleks dan melibatkan teknik APT (Advanced Persistent Threat) yang sulit dideteksi secara konvensional.

Di sisi lain, pendekatan kebijakan nasional juga masih bersifat reaktif. Banyak insiden kebocoran data tidak ditanggapi dengan pembaruan sistematis terhadap sistem keamanan digital, melainkan hanya diatasi sementara secara administratif [9]. Ini menunjukkan bahwa sistem mitigasi dan respons terhadap insiden digital belum menjadi bagian dari kerangka kebijakan pertahanan yang terintegrasi. Meski pemerintah telah meluncurkan roadmap transformasi digital di sektor pertahanan melalui kolaborasi antara Kemhan dan Kementerian BUMN, implementasinya belum menyentuh aspek interoperabilitas lintas BUMN pertahanan secara menyeluruh [10].

Melihat urgensi dan kompleksitas tantangan tersebut, penelitian ini bertujuan untuk mengevaluasi secara kritis peran DEFEND ID dalam pengembangan sistem informasi pertahanan yang aman, terintegrasi, dan berorientasi pada kemandirian nasional. Kajian ini tidak hanya mengulas sejauh mana transformasi digital telah dilakukan oleh perusahaan-perusahaan dalam DEFEND ID, tetapi juga menyodorkan alternatif strategi yang dapat memperkuat posisi Indonesia dalam ekosistem pertahanan digital global. Dengan mengedepankan model kolaborasi triple helix yang melibatkan akademisi, industri, dan pemerintah, diharapkan tercipta ekosistem pertahanan digital yang bukan hanya tangguh secara teknologi, tetapi juga berkelanjutan dan berbasis pada sumber daya dalam negeri.

2. TINJAUAN PUSTAKA

Sistem informasi memiliki peran strategis dalam organisasi modern, terlebih dalam institusi pertahanan yang mengelola informasi sensitif dan operasional berskala besar. Sistem informasi didefinisikan sebagai seperangkat komponen yang saling terhubung untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan informasi guna mendukung pengambilan keputusan, koordinasi, serta pengawasan dalam organisasi [3]. Dalam konteks pertahanan nasional, sistem ini tidak hanya mendukung fungsi administratif, tetapi juga menjadi sarana penting dalam pengendalian logistik militer, manajemen alutsista, komunikasi taktis, hingga deteksi dan penanganan ancaman siber [3].

Secara normatif, penguatan sistem informasi di sektor pertahanan telah memiliki dasar hukum yang kuat, yaitu Undang-Undang Nomor 16 Tahun 2012 tentang Industri Pertahanan. Dalam beleid ini, negara menegaskan pentingnya penguasaan teknologi strategis oleh industri dalam negeri sebagai kunci kemandirian pertahanan, termasuk dalam bidang teknologi informasi dan komunikasi [4]. Sayangnya, peraturan ini belum sepenuhnya diterjemahkan ke dalam strategi sistem informasi nasional yang terstandar, terintegrasi, dan aman terhadap intervensi asing.

Transformasi digital yang digagas oleh DEFEND ID sebagai holding BUMN industri pertahanan menjadi salah satu langkah konkret dalam menjawab tantangan tersebut. Sebagai contoh, PT LEN dan PT PAL mencatat peningkatan efisiensi distribusi logistik hingga 17% setelah mengimplementasikan sistem Enterprise Resource Planning (ERP) dan sistem informasi produksi [2]. PT Dahana pun telah menerapkan sistem Manufacturing Execution System (MES) yang terbukti meningkatkan akurasi data serta produktivitas lini produksi bahan peledak [5].

Namun, capaian ini masih bersifat sektoral dan belum berdampak sistemik karena tidak diiringi dengan integrasi antarsistem informasi antarperusahaan dalam DEFEND ID. Machmud, Almubaroq, dan Sarjito (2024) menyatakan bahwa strategi manajemen yang efektif di DEFEND ID mengarah pada pencapaian global dengan analisis

SWOT yang mempertimbangkan tantangan dan peluang teknologi dalam sistem pertahanan. [6]. Sementara itu, Wheelen dan Hunger menyebut bahwa pengelolaan informasi yang efektif merupakan fondasi untuk membentuk organisasi yang adaptif dan tahan terhadap perubahan lingkungan [7].

Kajian tambahan menunjukkan bahwa meskipun sistem informasi pertahanan berbasis satelit menawarkan keunggulan dalam mobilitas dan cakupan, sistem ini tetap memerlukan fondasi keamanan lokal seperti penggunaan server militer mandiri, teknologi enkripsi nasional, serta kebijakan tata kelola data yang kuat dan berdaulat [1]. Tanpa itu, kedaulatan informasi Indonesia rentan dieksploitasi melalui penyadapan dan manipulasi data yang dilakukan oleh aktor negara maupun non-negara.

Dalam hal kesiapan infrastruktur dan sumber daya manusia, BSSN melaporkan bahwa hanya 21% institusi pertahanan di Indonesia yang telah memiliki sistem mitigasi terhadap serangan siber tingkat tinggi seperti Advanced Persistent Threats (APT) [8]. Kondisi ini mencerminkan lemahnya kesadaran strategis terhadap risiko digital dan minimnya investasi pada pelatihan SDM yang kompeten di bidang keamanan informasi pertahanan.

Di sisi lain, media massa beberapa kali melaporkan kelemahan sistem keamanan nasional yang cenderung lambat dan reaktif dalam menangani kebocoran data pertahanan. Insiden peretasan dan penyusupan sistem sering kali tidak diikuti dengan investigasi forensik digital atau pembaruan sistem keamanan yang sistemik [9]. Ketidaksiapan dalam merespons ini berpotensi memperbesar kerugian strategis jangka panjang dan menurunkan kepercayaan publik terhadap kapasitas pertahanan negara.

Pemerintah melalui Kementerian Pertahanan dan Kementerian BUMN sebenarnya telah menyusun cetak biru transformasi digital pertahanan yang mencakup rencana interoperabilitas sistem informasi, integrasi data strategis, serta sinergi dengan sistem komunikasi berbasis satelit militer. Dokumen ini diharapkan dapat menjadi pijakan dalam membangun sistem pertahanan digital yang aman, responsif, dan mandiri [10]. Akan tetapi, sampai saat ini belum tersedia kajian evaluatif yang mengukur sejauh mana peta jalan ini telah diterapkan dan apa saja tantangan lapangan yang dihadapi.

Dari berbagai literatur tersebut dapat disimpulkan bahwa pengembangan sistem informasi pertahanan nasional tidak hanya soal adopsi teknologi canggih, tetapi juga menyangkut konsistensi regulasi, penguatan institusi pengelola, peningkatan kompetensi SDM, serta sinergi antara industri dan pemerintah. Tanpa kerangka tata kelola yang jelas dan sistem yang saling terhubung, sistem informasi pertahanan hanya akan menjadi proyek jangka pendek yang tidak mampu menjawab ancaman keamanan yang semakin kompleks dan digital.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode studi pustaka (library research), yang bertujuan untuk mendalami dinamika dan permasalahan sistem informasi pertahanan dalam konteks transformasi digital oleh holding industri pertahanan nasional, DEFEND ID. Pendekatan ini dipilih karena mampu memberikan pemahaman yang mendalam dan holistik terhadap suatu fenomena berdasarkan data yang telah tersedia, baik berupa dokumen, teori, maupun hasil penelitian terdahulu [2]. Teknik ini relevan digunakan ketika peneliti menghadapi keterbatasan akses terhadap data primer langsung, terutama dalam sektor strategis seperti pertahanan, namun tetap ingin menghasilkan analisis yang kritis dan terukur secara akademik [5].

3.1. Sumber Data

Sumber data dalam penelitian ini diperoleh dari sepuluh dokumen utama yang terdiri dari jurnal ilmiah, buku referensi sistem informasi, dokumen kebijakan publik terbaru dari Kementerian Pertahanan RI (2025), hasil kajian strategis perusahaan DEFEND ID, serta artikel dari media resmi nasional. Seluruh data dianalisis menggunakan pendekatan konten tematik, yaitu mengelompokkan informasi berdasarkan tema-tema utama yang muncul secara berulang, kemudian menguraikan hubungan antara tema tersebut dengan isu strategis yang diangkat dalam penelitian ini [3].

3.2. Teknik Analisis

Teknik analisis ini memfokuskan pada pencarian pola konseptual, hubungan sebab akibat, serta penyusunan argumen berdasarkan kedalaman makna dari teks yang dikaji. Proses analisis dilakukan melalui beberapa tahapan. Pertama, peneliti melakukan identifikasi awal terhadap indikator-indikator sistem informasi yang relevan dengan lingkungan pertahanan, berdasarkan kerangka teori yang dikemukakan oleh [3]. Indikator tersebut antara lain mencakup pengumpulan data, pengolahan, penyimpanan, distribusi informasi, serta peran teknologi dalam pengambilan keputusan organisasi. Kedua, kerangka kebijakan dianalisis berdasarkan Undang-Undang Nomor 16 Tahun 2012 serta cetak biru transformasi digital DEFEND ID, untuk melihat bagaimana regulasi tersebut diterjemahkan dalam aksi implementatif oleh BUMN pertahanan [4].

3.3. Analisis SWOT

Ketiga, peneliti melakukan analisis komparatif dengan menggunakan model SWOT terhadap strategi digital DEFEND ID, sebagaimana dikaji dalam dokumen resmi perusahaan [5]. Melalui pendekatan ini, peneliti dapat membandingkan antara kekuatan dan kelemahan internal sistem informasi, serta peluang dan ancaman eksternal yang dihadapi, khususnya dalam ranah keamanan data, kemandirian teknologi, dan tantangan interoperabilitas. Tahapan ini bertujuan untuk memetakan sejauh mana kesenjangan antara

kondisi aktual dan kerangka ideal penguatan sistem informasi pertahanan yang diharapkan.

3.4. Triangulasi Sumber

Untuk meningkatkan validitas temuan, penelitian ini menerapkan triangulasi sumber dengan cara membandingkan dan mengkonfirmasi data dari berbagai sudut pandang. Triangulasi dilakukan antara teori sistem informasi [3], dasar hukum dan kebijakan strategis [4], serta data SWOT yang mewakili kondisi aktual organisasi [5]. Pendekatan triangulatif ini penting untuk menghindari bias interpretasi dan memastikan bahwa simpulan yang dihasilkan memiliki basis argumen yang kuat secara ilmiah. Hasil dari analisis kemudian dikelompokkan ke dalam empat dimensi sistemik, yaitu efisiensi operasional sistem, kerentanan terhadap serangan siber, keterhubungan dan interoperabilitas antarsistem, serta arah kebijakan nasional dalam mendukung kemandirian sistem informasi pertahanan.

4. HASIL DAN PEMBAHASAN

Berdasarkan hasil analisis yang dilakukan, sistem informasi yang telah diimplementasikan oleh holding DEFEND ID memberikan kontribusi positif terhadap efisiensi operasional dan transparansi dalam sektor industri pertahanan nasional. Penerapan sistem Enterprise Resource Planning (ERP) di PT LEN dan Manufacturing Execution System (MES) di PT Dahana telah mempercepat pengambilan keputusan strategis, meminimalisasi kesalahan data, dan menurunkan biaya operasional yang sebelumnya disebabkan oleh duplikasi proses dan manajemen manual [2][5]. Efisiensi ini mencerminkan bahwa sistem informasi modern tidak hanya berperan sebagai alat bantu administratif, tetapi telah menjadi enabler utama dalam proses transformasi organisasi, sebagaimana ditekankan oleh [3]. Namun demikian, meskipun ada kemajuan yang dicapai, temuan penelitian ini juga mengidentifikasi sejumlah tantangan yang signifikan, terutama terkait dengan integrasi lintas institusi, keamanan data, sumber daya manusia, dan kolaborasi antar sektor.

4.1. Masalah Integrasi Lintas Institusi

Salah satu isu utama yang ditemukan dalam penelitian ini adalah fragmentasi sistem yang ada di lingkungan DEFEND ID. Meskipun masing-masing entitas seperti PT LEN, PT Dahana, dan PT PAL telah mengimplementasikan sistem ERP dan MES secara internal, sistem-sistem tersebut masih terisolasi (silo) dan tidak terintegrasi dengan baik. Hal ini menyebabkan ketidaksesuaian dalam pertukaran data strategis, yang sangat krusial dalam kondisi operasional gabungan yang memerlukan respons cepat dan akurat. Tanpa adanya standar interoperabilitas antar sistem, koordinasi antar entitas pertahanan berjalan secara manual dan sering kali redundan, yang pada akhirnya mengurangi efektivitas sistem pertahanan secara keseluruhan [1][4]. Rekomendasi: Penerapan standar interoperabilitas yang jelas dan pengembangan arsitektur sistem informasi terintegrasi di tingkat nasional akan meningkatkan efisiensi dan efektivitas koordinasi dalam operasi pertahanan.

4.2. Isu Keamanan

Keamanan data menjadi tantangan besar yang harus segera diatasi. Sebagian besar perangkat lunak sistem informasi yang digunakan oleh BUMN pertahanan masih bergantung pada teknologi asing, yang meningkatkan kerentanannya terhadap risiko penyadapan dan kebocoran data strategis. Serangan siber, terutama Advanced Persistent Threats (APT), semakin canggih dan berpotensi mengeksploitasi kerentanan pada sistem yang bergantung pada vendor luar negeri [8]. Dalam kondisi global yang tidak stabil, ketergantungan pada teknologi asing dapat membuka celah bagi musuh untuk mengekspos data penting dan merusak infrastruktur pertahanan negara. Rekomendasi: DEFEND ID harus segera membangun infrastruktur keamanan yang mandiri, termasuk pusat data militer nasional dengan sistem enkripsi yang kuat berbasis teknologi lokal. Pembentukan pusat data ini akan memperkuat ketahanan data pertahanan nasional.

4.3. Sumber Daya Manusia

Kompetensi sumber daya manusia (SDM) di sektor pertahanan juga menjadi masalah serius. Laporan dari BSSN menunjukkan bahwa hanya sekitar 21% hingga 30% dari SDM yang bekerja di sektor pertahanan yang memiliki sertifikasi atau pelatihan di bidang keamanan siber [8]. Kekurangan pelatihan dan keterampilan yang memadai ini berdampak pada lambatnya adopsi teknologi baru dan terbatasnya inovasi lokal dalam mengembangkan sistem informasi pertahanan yang berdaya saing tinggi. Rekomendasi: Perluasan program pelatihan dan sertifikasi keamanan siber bagi SDM di sektor pertahanan harus dilakukan untuk meningkatkan kemampuan mereka dalam mengantisipasi dan merespons ancaman digital yang semakin canggih.

4.4. Peluang dan Tantangan

DEFEND ID memiliki peluang strategis untuk menjadi pionir dalam pengembangan sistem informasi pertahanan yang mandiri dan terintegrasi. Sebagai holding yang menaungi seluruh BUMN pertahanan utama, DEFEND ID memiliki posisi yang kuat untuk mengembangkan ekosistem teknologi pertahanan yang lebih mandiri. Namun, untuk mewujudkan peran ini, DEFEND ID memerlukan dukungan kebijakan yang konsisten dari pemerintah, terutama dalam hal regulasi interoperabilitas, insentif untuk digitalisasi, dan alokasi anggaran untuk riset dan pengembangan (R&D) yang berkelanjutan [2][10]. Rekomendasi: Pemerintah perlu memberikan insentif untuk digitalisasi sektor pertahanan, memperkuat regulasi interoperabilitas nasional, serta mendukung pengembangan SDM dengan kerjasama antara pemerintah, industri, dan akademisi.

4.5. Kolaborasi Triple Helix

Kolaborasi antara pemerintah, industri, dan akademisi dalam mendukung transformasi digital sektor pertahanan masih terbatas. Namun, kolaborasi ini sangat penting untuk menghasilkan solusi teknologi yang tepat guna dan menciptakan kapasitas SDM yang memadai melalui program beasiswa, magang strategis, dan riset terapan. Tanpa sinergi antara ketiga sektor ini, sistem informasi pertahanan yang canggih sekalipun tidak akan dapat berfungsi optimal dalam konteks pertahanan negara. Rekomendasi: Pendekatan triple helix harus diperkuat dengan kolaborasi yang lebih intensif antara DEFEND ID, pemerintah, dan akademisi. Ini akan memastikan bahwa pengembangan sistem informasi pertahanan yang lebih efisien dan adaptif dapat tercapai dengan memanfaatkan inovasi terbaru dan memperkuat kapasitas SDM di sektor pertahanan.

4.6. Analisis SWOT

Dalam evaluasi sistem informasi DEFEND ID, analisis SWOT digunakan untuk menilai kekuatan, kelemahan, peluang, dan ancaman yang dihadapi dalam upaya digitalisasi pertahanan. Analisis ini memberikan gambaran mendalam mengenai posisi DEFEND ID dalam mengelola dan mengintegrasikan sistem informasi pertahanan nasional. Berikut adalah pembahasan lebih mendalam dari setiap elemen dalam analisis SWOT.

4.7. Kekuatan *(Strengths)*

- **ERP dan MES Terintegrasi [2][5]:** Sistem ERP (Enterprise Resource Planning) dan MES (Manufacturing Execution System) yang diterapkan di PT LEN dan PT Dahana adalah salah satu kekuatan utama DEFEND ID. Kedua sistem ini memungkinkan pengelolaan produksi dan distribusi logistik yang lebih efisien, yang pada gilirannya meningkatkan koordinasi operasional dan mempercepat pengambilan keputusan strategis. Integrasi antara sistem ERP dan MES juga mengurangi ketergantungan pada proses manual, meningkatkan akurasi data, dan mengurangi biaya operasional.
- **Dukungan Pemerintah [10]:** Sebagai holding BUMN pertahanan, DEFEND ID mendapat dukungan penuh dari pemerintah dalam hal kebijakan dan alokasi anggaran untuk digitalisasi sektor pertahanan. Kebijakan ini memberikan DEFEND ID keunggulan dalam hal akses terhadap teknologi, riset dan pengembangan, serta fasilitas untuk mempercepat transformasi digital.
- **Efisiensi Operasional [3]:** Implementasi teknologi informasi yang lebih baik memungkinkan perusahaan dalam grup DEFEND ID untuk mengoptimalkan proses bisnis mereka. Efisiensi yang tercapai, seperti peningkatan distribusi logistik hingga 17% dan penurunan biaya operasional hingga 12%, menunjukkan bahwa sistem informasi dapat berfungsi sebagai enabler yang sangat baik dalam sektor pertahanan.

4.8. Kelemahan *(Weakness)*

Meskipun sistem informasi yang ada di DEFEND ID telah berhasil meningkatkan efisiensi, ketergantungan pada teknologi asing masih menjadi kelemahan yang signifikan. Banyak sistem, perangkat lunak, dan perangkat keras yang digunakan masih bergantung pada vendor luar negeri. Ketergantungan ini tidak hanya meningkatkan biaya jangka panjang tetapi juga menambah kerentanannya terhadap serangan siber dan gangguan dari vendor asing yang mungkin memiliki kepentingan tertentu.

- **SDM yang Kurang Siap [8]:** Rendahnya kompetensi sumber daya manusia (SDM) dalam bidang keamanan siber di sektor pertahanan menjadi masalah besar. Laporan BSSN menunjukkan bahwa hanya sekitar 21% hingga 30% personel yang memiliki sertifikasi atau pengalaman di bidang ini. Kurangnya pelatihan dan keterampilan yang memadai pada personel pertahanan menyebabkan ketidakmampuan dalam mengantisipasi dan merespons ancaman siber yang semakin canggih dan beragam.
- **Fragmentasi Sistem [1]:** Meski telah ada upaya digitalisasi, sistem yang diterapkan oleh berbagai BUMN di bawah naungan DEFEND ID masih tidak terintegrasi dengan baik. Setiap entitas menggunakan sistem mereka sendiri yang tidak saling berhubungan. Hal ini menyebabkan kesulitan dalam berbagi informasi strategis antara perusahaan-perusahaan tersebut dan Kementerian Pertahanan, yang pada gilirannya memperlambat pengambilan keputusan dan mempengaruhi efektivitas operasi pertahanan secara keseluruhan.

4.9. Peluang (Opportunities)

- **Insentif TKDN Pertahanan [2]:** Pemerintah memberikan insentif bagi industri pertahanan yang dapat meningkatkan komponen dalam negeri, termasuk dalam pengembangan sistem informasi. DEFEND ID memiliki peluang besar untuk memanfaatkan insentif ini untuk mendorong pengembangan teknologi informasi dalam negeri, mengurangi ketergantungan pada produk asing, dan membangun ekosistem teknologi pertahanan yang lebih mandiri.
- **Kolaborasi dengan Kampus [6][8]:** Melalui pendekatan triple helix yang melibatkan pemerintah, industri, dan akademisi, DEFEND ID dapat mengembangkan inovasi yang lebih sesuai dengan kebutuhan sektor pertahanan. Kolaborasi dengan universitas dan lembaga penelitian dapat meningkatkan kualitas riset dan pengembangan (R&D), menciptakan teknologi yang lebih tepat guna dan sesuai dengan

karakteristik pertahanan Indonesia, sekaligus mempercepat pemenuhan kebutuhan SDM yang kompeten dalam teknologi informasi dan keamanan siber.

- **Tren Digital Global [7]:** Dengan kemajuan teknologi digital global, DEFEND ID memiliki peluang untuk memanfaatkan perkembangan teknologi terkini, seperti kecerdasan buatan (AI), big data, dan cloud computing, untuk memperkuat sistem informasi pertahanan. Penerapan teknologi canggih ini dapat memberikan keuntungan kompetitif dalam merespons ancaman dan mempercepat pengambilan keputusan dalam operasi pertahanan.

4.10. Ancaman *(Threats)*

- **Ancaman APT dan Serangan Siber [1]:** Ancaman siber semakin canggih, terutama dengan meningkatnya serangan menggunakan metode Advanced Persistent Threats (APT) yang dapat menembus pertahanan digital tradisional. Ketergantungan DEFEND ID pada teknologi dan sistem yang berasal dari luar negeri juga memperbesar kemungkinan serangan atau penyadapan oleh pihak asing. Ini menjadi ancaman nyata bagi keamanan data strategis pertahanan negara.
- **Embargo Teknologi [4]:** Jika ada ketegangan geopolitik atau kebijakan internasional yang membatasi akses Indonesia terhadap teknologi canggih, termasuk dalam sektor pertahanan, ini bisa mempengaruhi kemampuan DEFEND ID dalam mengembangkan dan memelihara sistem informasi yang dibutuhkan. Ketergantungan pada teknologi asing juga menambah kerentanannya terhadap embargos atau sanksi internasional.
- **Kebocoran Data [9]:** Tingginya frekuensi serangan siber, ditambah dengan ketidakmampuan sistem informasi untuk terintegrasi dengan baik, meningkatkan risiko kebocoran data strategis. Insiden kebocoran data yang terjadi di Kementerian Pertahanan menjadi contoh nyata betapa pentingnya mengamankan sistem informasi pertahanan nasional. Jika kebocoran data ini tidak segera diatasi, hal itu dapat mengancam keselamatan nasional dan memperlemah posisi pertahanan Indonesia.

4.11. Evaluasi Sistem Informasi Pertahanan DEFEND ID

Setelah melakukan analisis SWOT, langkah selanjutnya adalah mengevaluasi keberhasilan dan tantangan yang dihadapi dalam penerapan sistem informasi di DEFEND ID. Evaluasi ini melibatkan enam dimensi utama yang perlu diperhatikan: Infrastruktur, Interoperasi, Efisiensi, Keamanan, Sumber Daya Manusia, dan Kolaborasi.

- **Infrastruktur**
  Saat ini, sebagian besar infrastruktur yang digunakan oleh DEFEND ID masih bergantung pada teknologi asing. Untuk memastikan kedaulatan data dan informasi pertahanan, penting bagi DEFEND ID untuk membangun infrastruktur yang sepenuhnya berbasis teknologi dalam negeri. Ini termasuk pengembangan pusat data militer nasional yang dilengkapi dengan sistem enkripsi yang kuat dan berbasis teknologi lokal.
  Rekomendasi:
  Pembangunan pusat data yang mandiri dan peningkatan sistem enkripsi lokal dapat memperkuat ketahanan data pertahanan nasional.
- **Interoperasi**
  Sistem yang digunakan oleh DEFEND ID tidak memiliki standar interoperabilitas yang memadai. Hal ini menyebabkan kesulitan dalam berbagi data dan informasi antar berbagai entitas pertahanan, baik itu antar BUMN di bawah naungan DEFEND ID maupun dengan Kementerian Pertahanan.
  Rekomendasi:
  Menerapkan standar interoperabilitas yang jelas dan membangun arsitektur sistem informasi yang terintegrasi akan meningkatkan efisiensi dan efektivitas koordinasi dalam operasi pertahanan.
- **Efisiensi**
  Sistem ERP dan MES yang diterapkan di DEFEND ID telah terbukti meningkatkan efisiensi operasional, baik dalam hal produksi maupun distribusi logistik. Namun, masih ada ruang untuk meningkatkan penerapan digitalisasi dalam aspek-aspek lain, seperti manajemen alutsista dan pemantauan keamanan siber.
  Rekomendasi:
  Perluasan digitalisasi di seluruh lini proses bisnis dan operasional DEFEND ID dapat meningkatkan efisiensi lebih lanjut.
- **Keamanan**
  Keamanan data dan informasi strategis masih menjadi tantangan besar. Ketergantungan pada teknologi asing menambah kerentanannya terhadap ancaman siber, terutama dari serangan APT dan kebocoran data.
  Rekomendasi:
  DEFEND ID harus segera membangun sistem keamanan yang mandiri, dengan memperkuat enkripsi dan perlindungan data lokal. Pembentukan pusat data militer nasional dapat menjadi solusi untuk meningkatkan perlindungan terhadap data penting.
- **Sumber Daya Manusia**
  Sumber daya manusia yang kurang terampil dalam bidang keamanan siber menjadi hambatan dalam melindungi sistem informasi. Kurangnya pelatihan dan sertifikasi di bidang ini memengaruhi kemampuan sektor pertahanan

untuk mengantisipasi dan merespons ancaman siber.

Rekomendasi:

Program pelatihan dan sertifikasi keamanan siber bagi SDM di sektor pertahanan perlu diperluas untuk memastikan kesiapan dalam menghadapi ancaman digital.

- **Kolaborasi**

  Kolaborasi antara pemerintah, industri, dan akademisi dalam mendukung transformasi digital sektor pertahanan masih terbatas. Padahal, kerjasama antara ketiga pihak ini sangat penting untuk menciptakan solusi teknologi yang sesuai dengan kebutuhan pertahanan.

  Rekomendasi:

  Kolaborasi triple helix antara DEFEND ID, pemerintah, dan akademisi harus diperkuat untuk menciptakan sistem informasi pertahanan yang lebih efisien dan adaptif.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil pembahasan, penelitian ini menyimpulkan bahwa sistem informasi di lingkungan DEFEND ID telah memberikan kontribusi positif terhadap efisiensi operasional dan transparansi dalam sektor industri pertahanan nasional, terutama dalam hal pengelolaan logistik dan produksi. Penerapan sistem ERP di PT LEN dan MES di PT Dahana telah meningkatkan kecepatan pengambilan keputusan serta mengurangi biaya operasional. Namun, meskipun ada kemajuan dalam digitalisasi, integrasi antar-sistem informasi di DEFEND ID masih lemah dan tidak terstandarisasi secara nasional, yang menyebabkan terhambatnya koordinasi antar entitas pertahanan.

Keamanan data menjadi isu utama, di mana sebagian besar sistem informasi pertahanan masih bergantung pada teknologi asing. Ketergantungan ini membuka potensi serangan siber canggih, seperti Advanced Persistent Threats (APT), yang dapat mengancam keutuhan data strategis pertahanan. Dalam hal ini, penting untuk membangun infrastruktur keamanan lokal yang lebih kokoh, termasuk pusat data militer nasional yang dilindungi oleh sistem enkripsi buatan dalam negeri.

Selain itu, sektor sumber daya manusia di DEFEND ID juga menghadapi tantangan, dengan hanya sebagian kecil pegawai yang memiliki kompetensi di bidang keamanan informasi dan manajemen risiko siber. Hal ini memperlambat inovasi dan adaptasi terhadap teknologi baru yang diperlukan untuk menjaga keunggulan dalam menghadapi ancaman digital.

Peluang untuk meningkatkan sistem informasi pertahanan ada pada pengembangan kebijakan yang mendukung penggunaan teknologi dalam negeri, peningkatan kolaborasi antara pemerintah, industri, dan akademisi melalui pendekatan triple helix, serta pengembangan kapasitas SDM melalui pelatihan dan sertifikasi dalam bidang keamanan siber.

Kesimpulannya, meskipun ada beberapa kemajuan dalam digitalisasi industri pertahanan, DEFEND ID masih menghadapi tantangan besar dalam hal integrasi sistem, keamanan data, dan kualitas sumber daya manusia yang perlu segera ditangani agar pertahanan nasional dapat lebih tangguh dalam menghadapi ancaman digital.

Pemerintah harus segera membentuk pusat data militer nasional dengan sistem enkripsi berbasis teknologi lokal. DEFEND ID perlu mengembangkan platform sistem informasi mandiri dengan dukungan regulasi yang mendorong interoperabilitas dan penggunaan TKDN [4][10]. Program beasiswa dan sertifikasi bagi SDM TI pertahanan harus diperluas untuk menciptakan talenta keamanan siber dalam negeri [8].

Kolaborasi triple helix antara DEFEND ID, pemerintah, dan akademisi harus menjadi pilar dalam mendesain dan mengimplementasikan arsitektur sistem informasi pertahanan nasional yang tangguh, mandiri, dan adaptif terhadap ancaman masa depan [6][7].

DAFTAR PUSTAKA

[1] R. Wulandari, P. Suharto, A. Hendra, "Strategi Kementerian Pertahanan dalam Pengamanan T. L. Wheelen and J. D. Hunger, *Strategic Management and Business Policy*, 13th ed., Pearson, 2012. Sistem Informasi Berbasis Satelit Guna Menghadapi Cyberthreat," *JRPP*, vol. 8, no. 1, 2025.

[2] A. B. Priyono, "Strategi Transformasi Holding BUMN DEFEND ID dalam Percepatan Kemandirian Alat Peralatan Pertahanan dan Keamanan," *JEHSS*, vol. 7, no. 2, 2024.

[3] Priyono, A. B. (2024). *Strategi Transformasi Holding BUMN DEFEND ID dalam Percepatan Kemandirian Alat Peralatan Pertahanan dan Keamanan*. *Journal of Education, Humaniora and Social Sciences (JEHSS)*, 7(2), 1-12.

[4] Kementerian Pertahanan Republik Indonesia. (2025). *Strategi Membangun Ketangguhan Cybersecurity*.

[5] N. Machmud, H. Z. Almubaroq, A. Sarjito, "Defend ID's Strategic Management to be in The Top 50 Defence Global Company: SWOT Analysis of PT Dahana," *IJHESS*, vol. 4, no. 1, 2024.

[6] Machmud, N., Almubaroq, H. Z., & Sarjito, A. (2024). *Defend ID's Strategic Management to be in The Top 50 Defence Global Company: SWOT Analysis of PT Dahana*. *International Journal of Humanities Education and Social Sciences (IJHESS)*, 4(1), 1-14.

[7] Sutomo, A., Thamrin, S., Widodo, P., & Reksoprodjo, Y. (2025). *Membangun Ketahanan Digital: Pengembangan Model Strategi Pertahanan Siber Berbasis Manajemen Risiko*. *Temali: Jurnal Pembangunan Sosial*, 8(1), 1-15.

[8] BSSN, "Laporan Tahunan Keamanan Siber Nasional 2023."
[9] Kompas.com, "Situs Kemhan Diretas, Data Pegawai Dibocorkan," *Kompas*, 2 Nov. 2023.
[10] Kementerian Pertahanan RI, "Peran Satelit dalam Sistem Pertahanan Nasional," 2021.