



## KERANGKA STRATEGIS ADOPSI E-GOVERNMENT DALAM MENINGKATKAN EFISIENSI SEKTOR PERTAHANAN

**Aris Sarjito**

Program Studi Manajemen Pertahanan, Fakultas Manajemen Pertahanan,  
Universitas Pertahanan Republik Indonesia, Indonesia

E-mail correspondence: [arissarjito@gmail.com](mailto:arissarjito@gmail.com)

### **Abstract**

*The defense sector, vital for national security, often faces inefficiencies due to outdated processes and limited transparency. This research investigates how E-Government, leveraging digital technologies, can enhance operational efficiency in defense operations. The aim is to develop a strategic framework for E-Government adoption in the defense sector. Employing qualitative research methods using secondary data, the study analyzes existing literature, policy documents, and case studies to evaluate the current state of E-Government implementation. Findings reveal that while some defense organizations have successfully integrated E-Government solutions, challenges persist, including cybersecurity issues and resistance to change. Key factors influencing successful adoption include technological readiness, organizational culture, and policy support. The research identifies that developing a strategic framework involves formulating best practices, guidelines, and actionable recommendations to address these challenges. The proposed framework aims to enhance efficiency by incorporating insights from successful implementations and overcoming identified obstacles. The study concludes that a well-structured strategic framework is essential for effective E-Government adoption, offering a comprehensive approach to improving defense sector operations.*

**Keywords:** *defense sector efficiency; digital transformation; e-government; operational challenges; strategic framework*

### **Abstrak**

Sektor pertahanan, yang merupakan sektor penting bagi keamanan nasional, sering kali menghadapi inefisiensi karena proses yang ketinggalan jaman dan terbatasnya transparansi. Penelitian ini menyelidiki bagaimana E-Government, dengan memanfaatkan teknologi digital, dapat meningkatkan efisiensi operasional dalam operasi pertahanan. Tujuannya adalah untuk mengembangkan kerangka strategis untuk adopsi E-Government di sektor pertahanan. Dengan menggunakan metode penelitian kualitatif dengan menggunakan data sekunder, studi ini menganalisis literatur yang ada, dokumen kebijakan, dan studi kasus untuk mengevaluasi kondisi implementasi E-Government saat ini. Temuan mengungkapkan bahwa meskipun beberapa organisasi pertahanan telah berhasil mengintegrasikan solusi E-Government, tantangan masih tetap ada, termasuk masalah keamanan siber dan penolakan terhadap perubahan. Faktor-faktor kunci yang mempengaruhi keberhasilan adopsi meliputi kesiapan teknologi, budaya organisasi, dan dukungan kebijakan. Penelitian ini mengidentifikasi bahwa pengembangan kerangka strategis melibatkan perumusan praktik terbaik, pedoman, dan rekomendasi yang dapat ditindaklanjuti untuk mengatasi tantangan-tantangan ini. Kerangka kerja yang diusulkan bertujuan untuk meningkatkan efisiensi dengan menggabungkan wawasan dari keberhasilan implementasi dan mengatasi hambatan yang teridentifikasi. Studi ini menyimpulkan bahwa kerangka strategis yang terstruktur dengan baik sangat penting untuk implementasi E-Government yang efektif, yang menawarkan pendekatan komprehensif untuk meningkatkan operasi sektor pertahanan.

**Kata kunci:** efisiensi sektor pertahanan; e-Government; kerangka strategis; tantangan operasional; transformasi digital

## 1. Pendahuluan

Dalam beberapa tahun terakhir, implementasi inisiatif E-Government telah mendapatkan momentum yang signifikan di berbagai sektor, termasuk pertahanan. Integrasi teknologi digital ke dalam operasional pemerintahan menjanjikan peningkatan efisiensi, transparansi, dan akuntabilitas. Penelitian ini menggali penelitian mutakhir tentang kerangka strategis adopsi E-Government yang bertujuan untuk meningkatkan efisiensi operasional di sektor pertahanan.

Penerapan e-government di sektor pertahanan telah menjadi tren global yang bertujuan untuk meningkatkan efisiensi, transparansi, dan keamanan dalam pengelolaan sumber daya serta operasional militer. Menurut laporan United Nations E-Government Survey (2022), lebih dari 80% negara di dunia telah mengimplementasikan berbagai bentuk teknologi digital dalam sistem administrasi mereka, termasuk di sektor pertahanan. Di Indonesia, misalnya, Kementerian Pertahanan telah meluncurkan Sistem Informasi Pertahanan dan Keamanan (SISPAM) yang memfasilitasi koordinasi antara instansi militer dan sipil dalam rangka meningkatkan responsivitas dan pengambilan keputusan yang cepat (Brillianty, 2023).

Selain itu, e-government di sektor pertahanan juga mencakup penggunaan sistem manajemen sumber daya pertahanan yang memungkinkan pemantauan logistik, personel, dan aset militer secara real-time. Negara seperti Amerika Serikat telah menerapkan Defense Information Systems Agency (DISA), sebuah platform digital yang mendukung jaringan komunikasi global untuk memastikan kelancaran operasi militer (Vollmer, 2021). Penggunaan e-government dalam sektor pertahanan tidak hanya membantu dalam pengelolaan internal, tetapi juga meningkatkan ketahanan siber, yang penting dalam menghadapi ancaman modern. Data dari NATO menunjukkan bahwa serangan siber terhadap infrastruktur pertahanan meningkat hingga 300% dalam lima tahun terakhir, sehingga penerapan teknologi digital yang aman menjadi sangat penting (NATO REVIEW, 2021).

Sektor pertahanan, yang ditandai dengan kompleksitas dan kebutuhan akan langkah-langkah keamanan yang ketat, akan memperoleh manfaat yang sangat besar dari implementasi E-Government. Proses tradisional dalam operasi pertahanan sering kali melibatkan birokrasi yang signifikan, sehingga menyebabkan inefisiensi dan penundaan. Pengenalan E-Government dapat menyederhanakan proses-proses ini dengan mengotomatiskan tugas-tugas rutin, sehingga membebaskan sumber daya manusia untuk fungsi-fungsi yang lebih strategis (Kuhlmann & Marienfeldt, 2023).

Kerangka kerja strategis yang kuat untuk implementasi E-Government di sektor pertahanan harus memasukkan beberapa komponen penting untuk memastikan efektivitas dan efisiensi. Kerangka Tata Kelola dan Kebijakan: Menetapkan kebijakan dan struktur tata kelola yang jelas merupakan hal mendasar, yang melibatkan pengembangan pedoman peraturan, definisi peran, dan kepatuhan terhadap standar internasional (Huang et al., 2022). Pembangunan Infrastruktur: Berinvestasi dalam infrastruktur digital yang canggih, seperti jaringan komunikasi yang aman, pusat data, dan layanan cloud yang disesuaikan dengan kebutuhan pertahanan, sangat penting untuk mendukung inisiatif E-Government (Draheim et al., 2021). Tindakan Keamanan Siber: Mengingat sifat sensitif dari informasi pertahanan, implementasi protokol keamanan siber yang kuat sangatlah penting, termasuk audit keamanan rutin, pemantauan ancaman secara real-time, dan teknologi enkripsi canggih (KPMG, 2022). Pelatihan Sumber Daya Manusia: Transisi ke model E-Government membutuhkan angkatan kerja yang mahir dalam teknologi digital, sehingga memerlukan pelatihan berkelanjutan dan program pengembangan untuk membekali personel pertahanan dengan keterampilan yang diperlukan (Steingartner et al., 2021). Manajemen Perubahan: Mengatasi pergeseran budaya dari operasi tradisional ke digital melibatkan strategi manajemen perubahan yang komprehensif, termasuk keterlibatan pemangku kepentingan dan rencana komunikasi yang efektif, untuk memastikan keberhasilan implementasi E-Government (Tóth, 2023).

Beberapa negara telah membuat kemajuan penting dalam mengintegrasikan E-Government dalam sektor pertahanan mereka. Misalnya, Estonia, yang terkenal dengan tata kelola digitalnya yang canggih, telah berhasil menerapkan kerangka kerja E-Government komprehensif yang meningkatkan efisiensi operasional dalam operasi pertahanannya. Pendekatan Estonia mencakup sistem identitas digital yang kuat, pertukaran data yang aman, dan akses real-time terhadap sumber daya pertahanan (OECD, 2021).

Demikian pula Korea Selatan yang telah mengembangkan sistem E-Government canggih yang mendukung sektor pertahanannya. Pusat Data Terpadu Pertahanan negara ini mengkonsolidasikan berbagai data terkait pertahanan, memfasilitasi pengambilan keputusan dan alokasi sumber daya yang efisien (C. Kim & Kim, 2021).

Meskipun mempunyai potensi manfaat, implementasi E-Government di sektor pertahanan penuh dengan tantangan. Hal ini mencakup penolakan terhadap perubahan, biaya implementasi yang tinggi, dan kekhawatiran terhadap keamanan data. Untuk mengatasi tantangan-tantangan ini memerlukan pendekatan implementasi bertahap, dimulai dengan proyek percontohan untuk menunjukkan manfaat dan membangun kepercayaan pemangku kepentingan (NATO, 2022).

Selain itu, membina kolaborasi internasional dapat membantu berbagi praktik dan teknologi terbaik, sehingga mengurangi biaya implementasi dan meningkatkan langkah-langkah keamanan. Kemitraan dengan perusahaan teknologi sektor swasta juga dapat memberikan keahlian dan inovasi yang diperlukan (UNDP, 2021).

Implementasi strategis E-Government di sektor pertahanan menjanjikan peningkatan efisiensi operasional secara signifikan. Kerangka kerja strategis yang terdefinisi dengan baik yang membahas tata kelola, infrastruktur, keamanan siber, pelatihan sumber daya manusia, dan manajemen perubahan sangat penting untuk mewujudkan manfaat-manfaat ini. Dengan belajar dari studi kasus yang berhasil dan mengatasi tantangan-tantangan yang melekat, organisasi-organisasi pertahanan dapat memanfaatkan potensi penuh E-Government untuk meningkatkan kemampuan operasional mereka.

Sektor pertahanan, yang merupakan landasan keamanan nasional, sering kali mengalami inefisiensi yang disebabkan oleh proses birokrasi yang ketinggalan jaman, koordinasi yang buruk, dan terbatasnya transparansi. Dengan evolusi dinamika keamanan global, terdapat kebutuhan mendesak bagi sektor pertahanan untuk menggunakan solusi teknologi modern guna meningkatkan efisiensi operasional. E-Government, yang melibatkan implementasi teknologi digital dalam administrasi publik, memberikan peluang yang menjanjikan untuk menyederhanakan operasi pertahanan. Namun, keberhasilan implementasi E-Government di sektor ini penuh dengan tantangan yang signifikan, termasuk ancaman keamanan siber, resistensi terhadap perubahan organisasi, dan kompleksitas dalam mengintegrasikan teknologi baru dengan sistem yang sudah ada. Untuk mengatasi hambatan-hambatan ini dan memastikan implementasi dan keberlanjutan inisiatif E-Government, kerangka kerja strategis yang komprehensif sangat penting. Kerangka kerja seperti ini akan mengatasi tantangan-tantangan ini secara langsung dan memberikan pendekatan terstruktur untuk mengintegrasikan solusi E-Government secara efektif dalam sektor pertahanan (KPMG, 2022; Zimmerman et al., 2019).

Tujuan penelitian untuk mengembangkan kerangka strategis implementasi E-Government guna meningkatkan efisiensi sektor pertahanan adalah sebagai berikut: Pertama, untuk menganalisis keadaan implementasi E-Government di sektor pertahanan saat ini, yang bertujuan untuk memberikan penilaian komprehensif tentang bagaimana inisiatif-inisiatif ini berdampak pada peningkatan efisiensi sektor pertahanan. telah diintegrasikan ke dalam operasi pertahanan, mengidentifikasi keberhasilan dan bidang yang perlu ditingkatkan. Tujuan ini akan memperjelas kesenjangan yang ada saat ini dan menyoroti bidang-bidang yang perlu diatasi untuk meningkatkan efisiensi operasional (Kuhlmann & Marienfeldt, 2023). Kedua, untuk mengidentifikasi faktor-faktor penting yang mempengaruhi keberhasilan implementasi E-Government, tujuan ini berupaya untuk mengeksplorasi berbagai elemen seperti infrastruktur teknologi, budaya organisasi, dan kerangka kebijakan. Dengan memahami faktor-faktor yang mempengaruhi ini, penelitian ini akan mengembangkan strategi yang ditargetkan untuk mengatasi

tantangan dan mendorong adopsi yang efektif (Tóth, 2023). Terakhir, tujuannya adalah untuk mengembangkan kerangka strategis yang meningkatkan efisiensi operasional melalui E-Government. Hal ini melibatkan perumusan strategi komprehensif yang mengintegrasikan praktik terbaik, solusi inovatif, dan rekomendasi praktis untuk organisasi pertahanan. Kerangka kerja ini akan bertindak sebagai pedoman bagi para pembuat kebijakan dan praktisi, yang bertujuan untuk memanfaatkan E-Government guna mencapai peningkatan efisiensi dalam operasi pertahanan (Draheim et al., 2021).

Penelitian ini bertujuan untuk menjawab beberapa pertanyaan kritis untuk mengembangkan kerangka strategis yang efektif untuk adopsi E-Government di sektor pertahanan. Pertama, bagaimana implementasi E-Government di sektor pertahanan saat ini? Pertanyaan ini berupaya untuk membangun pemahaman dasar tentang bagaimana inisiatif E-Government diadopsi dalam operasi pertahanan, mengidentifikasi solusi digital yang ada, implementasinya, dan hasil yang dicapai hingga saat ini. Menjawab hal ini akan mengungkap studi kasus yang berhasil dan bidang-bidang yang memerlukan pengembangan lebih lanjut, memberikan wawasan mengenai integrasi teknologi digital dalam pertahanan saat ini (OECD, 2021). Kedua, apa saja faktor penting yang mempengaruhi keberhasilan implementasi E-Government di sektor pertahanan? Pertanyaan ini mengeksplorasi elemen spesifik yang berdampak pada implementasi E-Government, seperti kesiapan teknologi, langkah-langkah keamanan siber, budaya organisasi, dan dukungan kebijakan. Dengan memahami faktor-faktor ini, penelitian ini akan mengembangkan strategi untuk mengatasi tantangan unik yang dihadapi sektor pertahanan dalam mengadopsi solusi digital (J.-S. Kim et al., 2023). Yang terakhir, bagaimana kerangka strategis dapat dikembangkan untuk meningkatkan efisiensi operasional melalui E-Government di sektor pertahanan? Pertanyaan ini berfokus pada penciptaan kerangka strategis komprehensif yang mencakup praktik terbaik, pedoman, dan rekomendasi yang dapat ditindaklanjuti untuk mengintegrasikan E-Government ke dalam operasi pertahanan. Laporan ini bertujuan untuk menguraikan langkah-langkah yang dapat diambil oleh organisasi-organisasi pertahanan untuk meningkatkan efisiensi, memanfaatkan wawasan dari keberhasilan implementasi dan tantangan-tantangan yang teridentifikasi (UNDP, 2021).

Implementasi E-Government di sektor pertahanan mempunyai potensi yang signifikan untuk meningkatkan efisiensi operasional, transparansi, dan akuntabilitas. Namun, kompleksitas dan tantangan unik dalam lingkungan pertahanan memerlukan kerangka kerja strategis yang disusun secara cermat. Dengan mengatasi kondisi implementasi E-Government saat ini, mengidentifikasi faktor-faktor penting yang mempengaruhi, dan mengembangkan strategi komprehensif, penelitian ini bertujuan untuk memberikan wawasan berharga dan solusi praktis bagi organisasi pertahanan. Ketika dinamika keamanan global terus berkembang, implementasi transformasi digital melalui E-Government akan menjadi sangat penting untuk mempertahankan dan meningkatkan kemampuan operasional sektor pertahanan di seluruh dunia.

## **2. Metode**

Metode penelitian kualitatif menawarkan wawasan berharga terhadap fenomena kompleks dengan mengeksplorasi pola, tema, dan makna secara mendalam. Ketika memanfaatkan data sekunder, penelitian kualitatif menjadi alat yang ampuh untuk mengembangkan kerangka kerja strategis, khususnya dalam konteks seperti implementasi E-Government di sektor pertahanan. Menurut John W. Creswell, metode penelitian kualitatif dengan menggunakan data sekunder memberikan pendekatan yang kuat untuk memahami dan mengatasi nuansa kerangka strategis dengan memanfaatkan sumber informasi yang ada (Creswell, 2014). Penelitian ini membahas implementasi metode penelitian kualitatif Creswell dengan menggunakan data sekunder, disesuaikan dengan konteks pengembangan kerangka strategis adopsi E-Government yang bertujuan untuk meningkatkan efisiensi sektor pertahanan.

### **1. Pengertian Data Sekunder dalam Penelitian Kualitatif**

Data sekunder mengacu pada informasi yang dikumpulkan oleh peneliti selain peneliti yang saat ini menggunakannya. Data ini dapat mencakup studi yang dilakukan sebelumnya, laporan, dokumen

kebijakan, dan catatan sejarah. Creswell menekankan bahwa analisis data sekunder dalam penelitian kualitatif bermanfaat karena memungkinkan peneliti mengakses berbagai informasi tanpa memerlukan pengumpulan data primer (Creswell, 2014). Metode ini sangat berguna untuk menyelidiki fenomena yang ada dan memahami tren yang lebih luas, sehingga cocok untuk mengembangkan kerangka kerja strategis.

## **2. Langkah-Langkah Penelitian Kualitatif Menggunakan Data Sekunder**

**Pengumpulan dan Seleksi Data:** Langkah pertama dalam menggunakan data sekunder untuk penelitian kualitatif melibatkan identifikasi dan pemilihan sumber data yang relevan. Creswell menyoroti pentingnya memilih sumber yang kredibel, relevan, dan komprehensif (Creswell, 2014). Dalam konteks implementasi E-Government di sektor pertahanan, data sekunder yang relevan mungkin mencakup dokumen kebijakan, studi kasus, laporan pemerintah, dan studi penelitian sebelumnya mengenai transformasi digital dalam organisasi pertahanan.

Misalnya, menganalisis laporan dari departemen pertahanan dan organisasi internasional dapat memberikan wawasan mengenai inisiatif E-Government yang ada dan dampaknya terhadap efisiensi operasional. Dokumen seperti strategi transformasi digital Departemen Pertahanan AS atau kerangka manajemen logistik NATO dapat memberikan data berharga untuk mengembangkan kerangka strategis (DoD, 2022; NATO, 2022).

**Analisis data:** Setelah data sekunder dikumpulkan, Creswell menyarankan penggunaan analisis tematik untuk mengidentifikasi pola dan tema dalam data (Creswell, 2014). Hal ini melibatkan pengkodean data, mengkategorikannya ke dalam tema, dan menafsirkan temuan untuk menarik kesimpulan yang bermakna.

Dalam mengembangkan kerangka strategis untuk adopsi E-Government, analisis tematik mungkin mengungkapkan faktor-faktor kunci yang mempengaruhi keberhasilan implementasi, seperti kesiapan teknologi, budaya organisasi, dan dukungan kebijakan. Dengan menganalisis tema secara sistematis di berbagai dokumen dan laporan, peneliti dapat mengidentifikasi praktik terbaik dan tantangan umum, yang penting untuk merumuskan strategi yang efektif (Viana, 2021).

**Menafsirkan Temuan:** Menafsirkan temuan dari data sekunder melibatkan sintesis wawasan yang diperoleh dari analisis tematik dan menghubungkannya dengan tujuan penelitian. Creswell menekankan pentingnya mengontekstualisasikan temuan dalam kerangka dan tujuan penelitian tertentu (Creswell, 2013).

Misalnya, jika analisis mengungkapkan bahwa permasalahan keamanan siber merupakan tema yang sering muncul dalam literatur, wawasan ini dapat digunakan untuk menekankan perlunya langkah-langkah keamanan yang kuat dalam kerangka strategis. Demikian pula, jika resistensi organisasi diidentifikasi sebagai sebuah tantangan, kerangka kerja tersebut harus mengatasi strategi manajemen perubahan dan adaptasi budaya (KPMG, 2022).

**Mengembangkan Kerangka Strategis:** Berdasarkan wawasan yang diperoleh dari analisis data sekunder, peneliti dapat mengembangkan kerangka strategis yang menggabungkan praktik terbaik, pedoman, dan rekomendasi yang dapat ditindaklanjuti. Creswell mencatat bahwa pengembangan kerangka kerja tersebut harus bersifat berulang dan fleksibel, memungkinkan penyesuaian berdasarkan wawasan baru dan konteks yang terus berkembang (Creswell, 2014).

Misalnya, kerangka strategis untuk implementasi E-Government di sektor pertahanan mungkin mencakup komponen-komponen seperti rekomendasi kebijakan, pedoman integrasi teknologi, dan strategi untuk mengatasi hambatan organisasi. Kerangka kerja ini harus didasarkan pada tema-tema yang diidentifikasi dari data sekunder, dan memastikan kerangka ini menjawab kebutuhan dan tantangan spesifik sektor pertahanan (J.-S. Kim et al., 2023; Tóth, 2023).

Pemanfaatan data sekunder dalam penelitian kualitatif menawarkan beberapa keuntungan, antara lain efektivitas biaya, penghematan waktu, dan kemampuan mengakses berbagai informasi. Hal ini memungkinkan peneliti untuk membangun pengetahuan yang ada dan mengeksplorasi tren yang sudah

ada tanpa memerlukan pengumpulan data primer (Creswell, 2014). Namun, penelitian data sekunder juga memiliki keterbatasan, seperti potensi kesenjangan dalam relevansi data, informasi yang sudah ketinggalan zaman, dan kurangnya kendali terhadap kualitas data. Para peneliti harus mengevaluasi secara kritis reliabilitas dan validitas sumber-sumber sekunder untuk mengurangi keterbatasan ini dan memastikan kekokohan temuan mereka (Draheim et al., 2021).

### **3. Hasil dan Pembahasan**

#### **1. Implementasi E-Government Saat Ini di Sektor Pertahanan**

E-Government, yang didefinisikan sebagai penggunaan teknologi digital untuk meningkatkan penyampaian layanan dan operasional pemerintah, telah diterapkan secara signifikan di berbagai sektor publik. E-government sebagai sebuah upaya dan bentuk pelayanan berbasis digital yang diusahakan oleh pemerintah agar mencapai efisiensi (Cahyani and Putra, 2024). Di sektor pertahanan, di mana efisiensi, transparansi, dan keamanan adalah hal yang terpenting, implementasi inisiatif E-Government menawarkan peluang dan tantangan (Sarjito, 2024; Yang et al., 2019). Diskusi ini bertujuan untuk memberikan pemahaman komprehensif mengenai keadaan E-Government di sektor pertahanan saat ini dengan mengkaji solusi digital yang ada, bidang implementasinya, dan hasil yang dicapai hingga saat ini.

Cahyani, N.P.K. and Putra, I.P.A.P. (2024) 'Governance And Digital Transformation: Analisis Ruang Kerja Virtual Melalui Perspektif E-Government Pada Pemerintahan Provinsi Bali', *Public Sphere Review*, 3(1), pp. 1–11. Available at: <https://doi.org/10.30649/psr.v3i1.123>.

Integrasi E-Government ke dalam operasi pertahanan menampilkan beberapa solusi digital utama yang bertujuan untuk meningkatkan efisiensi dan pengambilan keputusan. Sistem Manajemen Pertahanan Terpadu telah menjadi lazim, mengkonsolidasikan berbagai fungsi manajemen ke dalam platform terpadu yang memungkinkan akses data waktu nyata dan pengelolaan sumber daya yang lebih baik. Contohnya adalah sistem Defense Enterprise Resource Planning (DERP) Departemen Pertahanan A.S., yang menggabungkan data keuangan, logistik, dan personel ke dalam satu kerangka kerja (Deloitte, 2021; DoD, 2022). Keamanan siber dan Sistem Jaminan Informasi juga penting, dengan solusi canggih diterapkan untuk melindungi informasi pertahanan sensitif melalui jaringan komunikasi yang aman dan teknologi enkripsi canggih (KPMG, 2022). Sistem Manajemen Logistik dan Rantai Pasokan Otomatis menyederhanakan proses pengadaan, melacak inventaris, dan memastikan pengiriman pasokan tepat waktu, seperti yang dicontohkan oleh sistem manajemen logistik otomatis NATO Support and Procurement Agency (NSPA), yang meningkatkan efisiensi rantai pasokan (NATO, 2023). Selain itu, Alat Pelatihan dan Simulasi Digital menyediakan alat canggih untuk pelatihan berbasis skenario, menawarkan simulasi realistis yang meningkatkan hasil pelatihan dan kesiapan operasional (Taliaferro et al., 2022). Solusi-solusi ini secara kolektif berkontribusi pada perampingan proses, peningkatan koordinasi, dan peningkatan kemampuan pengambilan keputusan dalam sektor pertahanan.

Implementasi E-Government dalam operasi pertahanan telah memberikan dampak besar pada beberapa bidang penting. Efisiensi Operasional telah mengalami peningkatan yang signifikan melalui otomatisasi tugas-tugas rutin dan alur kerja yang disederhanakan (Manoharan et al., 2021). Misalnya saja, sistem manajemen dokumen elektronik telah secara signifikan mengurangi dokumen dan mempercepat proses administrasi di dalam badan-badan pertahanan, sehingga menghasilkan operasi yang lebih efisien (Accenture, 2021). Pengambilan Keputusan Strategis telah ditingkatkan melalui analisis data tingkat lanjut dan akses informasi waktu nyata, yang memungkinkan badan-badan pertahanan menganalisis data dalam jumlah besar untuk perencanaan strategis yang lebih baik dan pengambilan keputusan yang lebih tepat waktu dan tepat waktu (Viana, 2021). Selain itu, Koordinasi Antar Lembaga telah meningkat dengan implementasi platform komunikasi terintegrasi dan sistem berbagi data. Solusi E-Government ini memfasilitasi koordinasi yang lebih baik di antara badan-badan pertahanan dan badan-badan pemerintah lainnya, sehingga meningkatkan efektivitas operasional secara

keseluruhan dan mendorong kolaborasi yang lancar (UNDP, 2021). Secara kolektif, aplikasi-aplikasi ini menggarisbawahi potensi transformatif E-Government dalam mengoptimalkan operasi pertahanan dan proses pengambilan keputusan.

Implementasi E-Government di sektor pertahanan telah membuahkan beberapa hasil positif yang penting. Peningkatan Efisiensi adalah salah satu manfaat utamanya, karena otomatisasi dan integrasi digital telah meningkatkan proses operasional secara signifikan. Misalnya, sistem Perencanaan Sumber Daya Perusahaan Pertahanan (DERP) milik Departemen Pertahanan (DoD) telah menyederhanakan pengelolaan keuangan dan sumber daya, sehingga menghasilkan penghematan biaya yang besar dan peningkatan alokasi sumber daya (DoD, 2022). Peningkatan Keamanan adalah hasil penting lainnya, dengan langkah-langkah keamanan siber tingkat lanjut yang memperkuat perlindungan informasi pertahanan sensitif. Implementasi jaringan komunikasi yang aman dan teknologi enkripsi telah secara efektif memitigasi risiko yang terkait dengan pelanggaran data dan ancaman dunia maya, serta memastikan integritas data pertahanan (KPMG, 2022). Selain itu, Peningkatan Pelatihan dan Kesiapsiagaan telah dicapai melalui alat pelatihan digital dan teknologi simulasi, yang menawarkan skenario pelatihan yang realistis. Alat-alat ini telah secara signifikan meningkatkan efektivitas program pelatihan pertahanan, yang mengarah pada kesiapsiagaan dan kesiapan operasional yang lebih baik (Taliaferro et al., 2022). Secara kolektif, hasil-hasil ini menggarisbawahi dampak transformatif E-Government terhadap efisiensi, keamanan, dan kesiapan operasi pertahanan.

Meskipun terdapat hasil positif yang dicapai melalui E-Government di sektor pertahanan, masih terdapat beberapa tantangan besar. Biaya Implementasi yang Tinggi menimbulkan hambatan besar, karena investasi finansial yang diperlukan untuk teknologi dan sistem baru bisa sangat besar, sehingga membatasi ruang lingkup implementasinya (Abusamhadana et al., 2021). Resistensi terhadap Perubahan di dalam organisasi semakin memperumit transisi ini, karena praktik yang mengakar dan skeptis terhadap transformasi digital dapat memperlambat atau menghambat kemajuan. Selain itu, Kompleksitas dalam Mengintegrasikan Teknologi Baru dengan sistem yang ada menimbulkan kesulitan teknis, sehingga memerlukan upaya dan sumber daya yang besar untuk memastikan kompatibilitas dan fungsionalitas. Selain itu, menjaga Keamanan Siber yang Kuat sambil mengelola sejumlah besar data sensitif tetap menjadi perhatian penting, karena sektor pertahanan harus melindungi terhadap ancaman siber yang terus berkembang dan pelanggaran data sambil memastikan integritas dan kerahasiaan informasinya. (Deloitte, 2021; KPMG, 2022). Tantangan-tantangan ini menyoroti perlunya strategi komprehensif untuk mengatasi hambatan keuangan, organisasi, dan teknis yang terkait dengan implementasi E-Government dalam operasi pertahanan.

E-Government, yang didefinisikan sebagai penggunaan teknologi digital untuk meningkatkan penyampaian layanan dan operasional pemerintah, telah diterapkan secara signifikan di berbagai sektor publik. Di sektor pertahanan, di mana efisiensi, transparansi, dan keamanan adalah hal yang terpenting, implementasi inisiatif E-Government menawarkan peluang dan tantangan (Sarjito, 2024; Yang et al., 2019).

Integrasi E-Government ke dalam operasi pertahanan menampilkan beberapa solusi digital utama yang bertujuan untuk meningkatkan efisiensi dan pengambilan keputusan. Solusi-solusi ini, beserta implementasi dan dampak spesifiknya, dirangkum dalam tabel di bawah.

**Tabel 1.**  
Implementasi E-Government Saat Ini di Sektor Pertahanan

<b>Kategori</b>	<b>Detail</b>	<b>Referensi</b>
Solusi Digital yang Ada	Sistem Manajemen Pertahanan Terintegrasi: Platform terpadu untuk akses data real-time dan manajemen sumber daya. Contoh: sistem DERP Departemen Pertahanan.	(Deloitte, 2021; DoD, 2022)
	Sistem Keamanan Siber dan Jaminan Informasi: Solusi canggih untuk melindungi integritas dan kerahasiaan data.	(KPMG, 2022)

	Logistik Otomatis dan Manajemen Rantai Pasokan: Sistem untuk mengelola pengadaan, inventaris, dan efisiensi rantai pasokan. Contoh: manajemen logistik otomatis NATO.	(NATO, 2023)
	Alat Pelatihan dan Simulasi Digital: Alat untuk pelatihan berbasis skenario dan peningkatan kesiapan operasional.	(Taliaferro et al., 2022)
Area Aplikasi	Efisiensi Operasional: Otomatisasi dan alur kerja digital mengurangi dokumen dan mempercepat proses.	(Accenture, 2021)
	Pengambilan Keputusan Strategis: Peningkatan analisis data dan informasi real-time meningkatkan pengambilan keputusan.	(Viana, 2021)
	Koordinasi Antar-Lembaga: Koordinasi dan kolaborasi yang lebih baik antara pertahanan dan badan-badan pemerintah lainnya.	(UNDP, 2021)
Hasil yang Dicapai	Peningkatan Efisiensi: Otomatisasi menghasilkan peningkatan pengelolaan sumber daya dan penghematan biaya. Contoh: sistem DERP Departemen Pertahanan.	(DoD, 2022)
	Keamanan yang Ditingkatkan: Langkah-langkah keamanan siber tingkat lanjut melindungi informasi sensitif dan memitigasi risiko.	(KPMG, 2022)
	Peningkatan Pelatihan dan Kesiapsiagaan: Simulasi realistis meningkatkan hasil dan kesiapan pelatihan.	(Taliaferro et al., 2022)
Tantangan dan Keterbatasan	Biaya Implementasi Tinggi: Diperlukan investasi finansial yang signifikan untuk teknologi baru.	(Deloitte, 2021; KPMG, 2022)
	Resistensi terhadap Perubahan: Kelambanan organisasi dan resistensi budaya terhadap transformasi digital.	(Deloitte, 2021)
	Kompleksitas Integrasi: Kesulitan dalam mengintegrasikan teknologi baru dengan sistem yang sudah ada.	(KPMG, 2022)
	Masalah Keamanan Siber: Mengelola data sensitif dalam jumlah besar sambil memastikan langkah-langkah keamanan yang kuat.	(Deloitte, 2021; KPMG, 2022)

Sumber: diolah oleh Penulis, 2024.

Implementasi E-Government dalam operasi pertahanan telah memberikan dampak besar pada beberapa bidang penting. Efisiensi operasional telah mengalami peningkatan yang signifikan melalui otomatisasi tugas-tugas rutin dan alur kerja yang disederhanakan (Manoharan et al., 2021). Pengambilan keputusan strategis telah ditingkatkan melalui analisis data tingkat lanjut dan akses informasi waktu nyata, yang memungkinkan badan-badan pertahanan menganalisis data dalam jumlah besar untuk perencanaan strategis yang lebih baik serta pengambilan keputusan yang lebih tepat dan tepat waktu (Liu, 2022). Selain itu, koordinasi antar-lembaga telah meningkat dengan implementasi platform komunikasi terpadu dan sistem berbagi data, yang memfasilitasi koordinasi yang lebih baik di antara lembaga-lembaga pertahanan dan dengan badan-badan pemerintah lainnya (Pickering & Fox, 2022).

Implementasi E-Government di sektor pertahanan telah menghasilkan beberapa hasil positif yang penting, seperti peningkatan efisiensi, peningkatan keamanan, dan peningkatan pelatihan dan kesiapsiagaan. Namun, masih terdapat beberapa tantangan besar, termasuk biaya implementasi yang tinggi, penolakan terhadap perubahan dalam organisasi, kompleksitas dalam mengintegrasikan teknologi baru dengan sistem yang ada, dan menjaga keamanan siber yang kuat sekaligus mengelola data sensitif dalam jumlah besar (Deloitte, 2021; KPMG, 2022). Tantangan-tantangan ini menyoroti perlunya strategi



komprehensif untuk mengatasi hambatan keuangan, organisasi, dan teknis yang terkait dengan implementasi E-Government dalam operasi pertahanan.

## **2. Strategi Adopsi Ideal E-Government di Sektor Pertahanan**

Menjawab pertanyaan kritis yang diangkat dalam pendahuluan, adopsi E-Government di sektor pertahanan memerlukan strategi komprehensif dan terukur. Pendekatan bertahap dan terstruktur diperlukan untuk mengurangi resistensi perubahan dan mengelola risiko keamanan, dengan proyek percontohan sebagai langkah awal guna menguji efektivitas teknologi dan membangun kepercayaan (Draheim et al., 2021). Peningkatan kesiapan infrastruktur sangat penting, dengan pengembangan sistem komunikasi terenkripsi dan platform cloud yang disesuaikan dengan kebutuhan operasional pertahanan (Draheim et al., 2021). Peningkatan kapabilitas keamanan siber menjadi prioritas untuk melindungi informasi sensitif melalui pemantauan ancaman real-time dan teknologi enkripsi mutakhir (KPMG, 2022). Selain itu, pengembangan sumber daya manusia melalui pelatihan berkelanjutan diperlukan untuk meningkatkan kompetensi personel dalam mengoperasikan teknologi digital (Steingartner et al., 2021). Kolaborasi internasional juga penting untuk berbagi praktik terbaik dan teknologi yang efektif, mengurangi biaya, serta meningkatkan ketahanan sistem (OECD, 2021). Dengan strategi ini, E-Government dapat meningkatkan efisiensi, responsivitas, dan mengurangi birokrasi di sektor pertahanan.

## **3. Faktor-Faktor Penting yang Mempengaruhi Keberhasilan Adopsi E-Government di Sektor Pertahanan**

Implementasi E-Government di sektor pertahanan menawarkan manfaat besar, termasuk peningkatan efisiensi operasional, peningkatan pengambilan keputusan, dan proses yang disederhanakan. Namun, sejumlah faktor penting berperan dalam keberhasilan implementasi inisiatif digital ini. Faktor-faktor ini mencakup kesiapan teknologi, langkah-langkah keamanan siber, budaya organisasi, dan dukungan kebijakan. Pemahaman elemen-elemen ini penting untuk mengembangkan strategi yang menjamin implementasi E-Government yang efektif dan realisasi potensi manfaatnya.

**Kesiapan Teknologi:** Kesiapan teknologi merupakan faktor mendasar yang mempengaruhi keberhasilan implementasi E-Government. Sektor pertahanan memerlukan infrastruktur digital yang canggih untuk mendukung operasi yang kompleks dan memastikan interoperabilitas antar berbagai sistem. Hal ini mencakup jaringan berkecepatan tinggi, solusi penyimpanan data yang andal, dan layanan cloud yang skalabel. Kemajuan terkini, seperti komputasi awan dan analisis data besar, telah merevolusi implementasi E-Government dengan menawarkan solusi yang terukur dan fleksibel. Misalnya, Departemen Pertahanan AS telah berinvestasi pada platform berbasis cloud untuk meningkatkan pengelolaan data dan ketangkasan operasional (DoD, 2022). Namun, mencapai kesiapan teknologi memerlukan investasi besar dan peningkatan berkelanjutan untuk mengimbangi kemajuan teknologi (Draheim et al., 2021).

**Langkah-langkah Keamanan Siber:** Mengingat sensitivitas informasi pertahanan, langkah-langkah keamanan siber yang kuat sangatlah penting. Sektor pertahanan adalah target utama serangan siber, dan memastikan keamanan sistem dan data digital merupakan tantangan besar (Chivukula et al., 2021). Langkah-langkah keamanan siber yang efektif mencakup implementasi teknologi enkripsi canggih, saluran komunikasi yang aman, dan audit keamanan rutin.

Misalnya, penggunaan jaringan komunikasi aman dan sistem pemantauan ancaman real-time oleh NATO menggambarkan pentingnya keamanan siber dalam inisiatif E-Government (NATO, 2023). Selain itu, mengembangkan strategi keamanan siber yang proaktif untuk mengatasi ancaman dan kerentanan yang muncul sangat penting untuk melindungi data pertahanan penting (Accenture, 2021).

**Budaya Organisasi:** Budaya organisasi memainkan peran penting dalam implementasi E-Government. Transisi ke sistem digital sering kali memerlukan perubahan budaya dalam organisasi pertahanan. Resistensi terhadap perubahan, kurangnya keterampilan digital, dan praktik birokrasi yang

sudah mendarah daging dapat menghambat keberhasilan implementasi inisiatif E-Government (Viana, 2021).

Mempromosikan budaya yang merangkul transformasi digital sangatlah penting. Hal ini mencakup investasi dalam program pelatihan untuk mengembangkan kompetensi digital di kalangan personel, mengembangkan lingkungan yang mendukung inovasi, dan mengatasi kekhawatiran terkait perpindahan pekerjaan. Komitmen kepemimpinan dan komunikasi yang jelas mengenai manfaat dan tujuan E-Government juga penting dalam mengatasi penolakan dan mendorong perubahan budaya (UNDP, 2021).

**Dukungan Kebijakan:** Dukungan kebijakan merupakan faktor penting lainnya yang mempengaruhi keberhasilan implementasi E-Government. Kebijakan yang jelas dan mendukung memberikan kerangka kerja untuk implementasi dan memastikan keselarasan dengan tujuan strategis yang lebih luas. Hal ini termasuk menetapkan pedoman peraturan, mendefinisikan peran dan tanggung jawab, dan mengamankan pendanaan untuk proyek-proyek E-Government (Malodia et al., 2021). Dukungan kebijakan yang efektif juga melibatkan kolaborasi antara lembaga pertahanan dan badan pemerintah lainnya untuk memastikan koherensi dan interoperabilitas sistem digital. Misalnya, kerangka kebijakan komprehensif yang menangani privasi data, standar interoperabilitas, dan proses pengadaan dapat memfasilitasi integrasi E-Government yang lebih lancar (Turner et al., 2022).

**Integrasi dan Interoperabilitas:** Integrasi dan interoperabilitas antara sistem yang ada dan sistem baru sangat penting untuk keberhasilan implementasi E-Government. Organisasi pertahanan sering kali beroperasi dengan sistem lama yang harus diintegrasikan dengan solusi digital modern. Memastikan kompatibilitas dan pertukaran data yang lancar antar sistem yang berbeda sangat penting untuk efisiensi operasional (Draheim et al., 2021).

Mengembangkan protokol dan antarmuka standar dapat mengatasi tantangan integrasi. Misalnya, inisiatif Uni Eropa untuk menciptakan platform digital yang dapat dioperasikan untuk operasi pertahanan menggambarkan pentingnya standarisasi dalam mencapai E-Government yang efektif (OECD, 2021).

Implementasi E-Government di sektor pertahanan menawarkan manfaat besar, termasuk peningkatan efisiensi operasional, peningkatan pengambilan keputusan, dan proses yang disederhanakan (Almamy, 2022). Namun, ada beberapa faktor penting yang berperan dalam keberhasilan implementasi inisiatif digital ini. Faktor-faktor ini mencakup kesiapan teknologi, langkah-langkah keamanan siber, budaya organisasi, dukungan kebijakan, serta integrasi dan interoperabilitas. Pemahaman elemen-elemen ini penting untuk mengembangkan strategi yang menjamin implementasi E-Government yang efektif dan realisasi potensi manfaatnya. Tabel di bawah ini merangkum faktor-faktor penting yang diidentifikasi dalam tinjauan literatur:

**Tabel 2.**

Faktor-Faktor Penting yang Mempengaruhi Keberhasilan Adopsi E-Government di Sektor Pertahanan

<b>Faktor</b>	<b>Keterangan</b>	<b>Contoh/Referensi</b>
Kesiapan Teknologi	Infrastruktur digital canggih, jaringan berkecepatan tinggi, penyimpanan data yang andal, layanan cloud yang skalabel.	Investasi Departemen Pertahanan AS pada platform berbasis cloud (DoD, 2022); peningkatan berkelanjutan (Draheim et al., 2021).
Tindakan Keamanan Siber	Implementasi enkripsi tingkat lanjut, saluran komunikasi yang aman, audit keamanan rutin, strategi keamanan siber yang proaktif.	Jaringan komunikasi aman NATO dan sistem pemantauan ancaman real-time (NATO, 2023); strategi keamanan siber (Accenture, 2021).
Budaya organisasi	Pergeseran budaya untuk merangkul transformasi digital, investasi dalam program pelatihan, mendorong inovasi, mengatasi masalah	Mengembangkan kompetensi digital; mengatasi perlawanan dan mendorong perubahan budaya (UNDP, 2021).

---

	perpindahan kerja, dan komitmen kepemimpinan.	
Dukungan Kebijakan	Menetapkan pedoman peraturan, menetapkan peran dan tanggung jawab, mengamankan pendanaan, memastikan koherensi dan interoperabilitas sistem digital.	Kerangka kebijakan yang menangani privasi data, standar interoperabilitas, proses pengadaan (Turner et al., 2022).
Integrasi dan Interoperabilitas	Memastikan kompatibilitas dan pertukaran data yang lancar antara sistem lama dan modern, mengembangkan protokol dan antarmuka standar.	Platform digital Uni Eropa yang dapat dioperasikan untuk operasi pertahanan (OECD, 2021); mengatasi tantangan integrasi (Draheim et al., 2021).

---

Sumber: diolah oleh Penulis, 2024

Tabel ini merangkum elemen-elemen kunci yang mempengaruhi keberhasilan implementasi E-Government di sektor pertahanan, memberikan gambaran yang jelas tentang faktor-faktor penting yang diperoleh dari literatur. Dengan memahami dan mengatasi faktor-faktor ini, organisasi pertahanan dapat mengembangkan strategi yang kuat untuk memastikan implementasi yang efektif dan keberlanjutan inisiatif E-Government.

#### **4. Mengembangkan Kerangka Strategis untuk Meningkatkan Efisiensi Operasional melalui E-Government di Sektor Pertahanan**

Di sektor pertahanan, efisiensi operasional sangat penting untuk menjaga keamanan nasional dan merespons ancaman yang muncul secara efektif. Integrasi E-Government menawarkan potensi yang signifikan untuk meningkatkan efisiensi dengan menyederhanakan proses, meningkatkan koordinasi, dan memungkinkan pengambilan keputusan yang lebih baik. Mengembangkan kerangka strategis untuk implementasi E-Government melibatkan penciptaan pendekatan terstruktur yang menggabungkan praktik terbaik, pedoman, dan rekomendasi. Diskusi ini mengeksplorasi bagaimana kerangka kerja tersebut dapat dirumuskan, memanfaatkan keberhasilan implementasi dan mengatasi tantangan-tantangan bersama.

#### **5. Komponen Utama Kerangka Strategis**

**Penilaian dan Perencanaan:** Langkah pertama dalam mengembangkan kerangka strategis adalah melakukan penilaian menyeluruh terhadap operasi saat ini dan kemampuan teknologi. Hal ini mencakup evaluasi sistem yang ada, mengidentifikasi inefisiensi, dan memahami kebutuhan spesifik sektor pertahanan (Chu & Xu, 2024). Berdasarkan penilaian ini, rencana rinci harus dirumuskan yang menguraikan tujuan adopsi E-Government, sumber daya yang diperlukan, dan jadwal pelaksanaannya (Viana, 2021).

Misalnya, Departemen Pertahanan (DoD) A.S. melakukan tinjauan komprehensif terhadap infrastruktur digitalnya untuk mengembangkan sistem Perencanaan Sumber Daya Perusahaan Pertahanan (DERP), yang mengintegrasikan berbagai aspek operasional ke dalam satu platform terpadu (Dawson, 2023). Penilaian tersebut memberikan dasar yang jelas dan memandu arah strategis inisiatif E-Government.

**Tata Kelola dan Pengembangan Kebijakan:** Tata kelola dan pengembangan kebijakan yang efektif sangat penting untuk keberhasilan implementasi E-Government. Penetapan struktur tata kelola mencakup penetapan peran dan tanggung jawab, penetapan mekanisme pengawasan, dan memastikan kepatuhan terhadap peraturan terkait (Antoni et al., 2024). Pengembangan kebijakan harus mengatasi bidang-bidang utama seperti privasi data, keamanan siber, dan standar interoperabilitas.

Misalnya, pembentukan kerangka kebijakan komprehensif pertahanan digital yang dilakukan oleh NATO menggambarkan pentingnya memiliki pedoman dan standar yang jelas untuk memandu inisiatif E-Government (Lněnička & Máchová, 2022). Kerangka kerja ini juga harus mencakup ketentuan untuk tinjauan dan pembaruan kebijakan secara berkala guna beradaptasi dengan perkembangan teknologi dan lanskap keamanan.

**Integrasi Infrastruktur dan Teknologi:** Investasi pada infrastruktur digital yang kuat sangat penting untuk mendukung inisiatif E-Government. Hal ini mencakup peningkatan sistem yang ada, implementasi teknologi canggih, dan memastikan interoperabilitas antara sistem baru dan lama (Saleh et al., 2021). Integrasi teknologi harus fokus pada penciptaan solusi yang terukur dan fleksibel yang dapat beradaptasi dengan kebutuhan masa depan.

Keberhasilan implementasi komputasi awan dan analisis data besar oleh berbagai organisasi pertahanan menyoroti manfaat modernisasi infrastruktur teknologi (Sreedevi et al., 2022). Teknologi tersebut memungkinkan pemrosesan data secara real-time dan meningkatkan ketangkasan operasional, yang sangat penting untuk operasi pertahanan.

**Keamanan Siber dan Manajemen Risiko:** Keamanan siber merupakan aspek penting dari E-Government di sektor pertahanan karena sensitivitas informasi yang terlibat. Mengembangkan strategi keamanan siber yang komprehensif melibatkan implementasi enkripsi tingkat lanjut, saluran komunikasi yang aman, dan pemantauan berkelanjutan terhadap potensi ancaman (Υφαντής, 2024). Praktik manajemen risiko juga harus ditetapkan untuk mengidentifikasi, menilai, dan memitigasi risiko yang terkait dengan operasi digital.

Misalnya, implementasi sistem deteksi ancaman real-time dan audit keamanan rutin oleh organisasi seperti Uni Eropa menggambarkan praktik terbaik dalam manajemen keamanan siber (Nwobodo et al., 2024). Memastikan langkah-langkah perlindungan yang kuat membantu menjaga integritas dan kerahasiaan informasi pertahanan.

**Pelatihan dan Manajemen Perubahan:** Implementasi E-Government yang sukses memerlukan fokus pada pelatihan dan manajemen perubahan. Personil harus dibekali dengan keterampilan digital yang diperlukan untuk menggunakan sistem dan teknologi baru secara efektif. Program pelatihan harus dirancang untuk mengatasi keterampilan teknis dan manajemen perubahan organisasi (Inakefe et al., 2023).

Kepemimpinan dan komunikasi yang jelas adalah komponen kunci manajemen perubahan. Melibatkan pemangku kepentingan dan mengatasi kekhawatiran terkait perpindahan pekerjaan dan perubahan operasional dapat memfasilitasi transisi yang lebih lancar (Brones et al., 2021). Misalnya, inisiatif transformasi digital Angkatan Darat A.S. mencakup pelatihan ekstensif dan program dukungan untuk memastikan keberhasilan adopsi teknologi baru.

**Pemantauan dan Evaluasi:** Menetapkan mekanisme untuk memantau dan mengevaluasi efektivitas inisiatif E-Government sangat penting untuk memastikan perbaikan berkelanjutan. Hal ini melibatkan penetapan metrik kinerja, melakukan evaluasi rutin, dan mengumpulkan umpan balik dari pengguna (Yıldırım & Bostancı, 2021).

Misalnya, Layanan Digital Pertahanan (DDS) di Departemen Pertahanan A.S. secara berkala menilai dampak inisiatif digitalnya untuk memastikan inisiatif tersebut memenuhi tujuan operasional dan mengidentifikasi area yang perlu ditingkatkan (Abiodun et al., 2021). Tinjauan rutin membantu menyempurnakan strategi dan meningkatkan efektivitas upaya E-Government secara keseluruhan.

Di sektor pertahanan, efisiensi operasional sangat penting untuk menjaga keamanan nasional dan merespons ancaman yang muncul secara efektif. Integrasi E-Government menawarkan potensi yang signifikan untuk meningkatkan efisiensi dengan menyederhanakan proses, meningkatkan koordinasi, dan memungkinkan pengambilan keputusan yang lebih baik. Mengembangkan kerangka strategis untuk adopsi E-Government melibatkan penciptaan pendekatan terstruktur yang menggabungkan praktik terbaik, pedoman, dan rekomendasi (Firman et al., 2023). Diskusi ini mengeksplorasi bagaimana kerangka kerja tersebut dapat dirumuskan, memanfaatkan keberhasilan implementasi dan mengatasi

tantangan-tantangan bersama. Tabel di bawah ini menguraikan komponen-komponen utama kerangka strategis untuk meningkatkan efisiensi operasional melalui E-Government di sektor pertahanan:

**Tabel 3.**  
Komponen Utama Kerangka Strategis untuk Meningkatkan Efisiensi Operasional Melalui E-Government di Sektor Pertahanan

<b>Komponen</b>	<b>Keterangan</b>	<b>Contoh/Referensi</b>
Penilaian dan Perencanaan	Melakukan penilaian menyeluruh terhadap operasi saat ini dan kemampuan teknologi; merumuskan rencana rinci yang menguraikan tujuan, sumber daya, dan jadwal.	Sistem Perencanaan Sumber Daya Perusahaan Pertahanan (DERP) Departemen Pertahanan A.S (Dawson, 2023); arah strategis (Viana, 2021).
Tata Kelola dan Pengembangan Kebijakan	Menetapkan struktur tata kelola dengan peran dan tanggung jawab yang jelas, menetapkan mekanisme pengawasan, dan mengembangkan kebijakan yang menangani privasi data, keamanan siber, dan interoperabilitas.	Kerangka kebijakan NATO untuk pertahanan digital (Lněnička & Máchová, 2022); tata kelola dan kepatuhan (Antoni et al., 2024).
Integrasi Infrastruktur dan Teknologi	Berinvestasi dalam infrastruktur digital yang kuat, tingkatkan sistem, terapkan teknologi canggih, dan pastikan interoperabilitas antara sistem baru dan lama.	Modernisasi melalui komputasi awan dan analisis data besar (Sreedevi et al., 2022); solusi terukur dan fleksibel (Saleh et al., 2021).
Keamanan Siber dan Manajemen Risiko	Mengembangkan strategi keamanan siber yang komprehensif, termasuk enkripsi tingkat lanjut, saluran komunikasi yang aman, pemantauan berkelanjutan, dan praktik manajemen risiko.	Deteksi ancaman dan audit keamanan secara real-time (Nwobodo et al., 2024); strategi keamanan siber (Υφαντής, 2024).
Keamanan Siber dan Manajemen Risiko	Mengembangkan strategi keamanan siber yang komprehensif, termasuk enkripsi tingkat lanjut, saluran komunikasi yang aman, pemantauan berkelanjutan, dan praktik manajemen risiko.	Deteksi ancaman dan audit keamanan secara real-time (Nwobodo et al., 2024); strategi keamanan siber (Υφαντής, 2024).
Pelatihan dan Manajemen Perubahan	Fokus pada pelatihan personel dalam keterampilan digital dan mengelola perubahan organisasi; merancang program yang menangani keterampilan teknis dan manajemen perubahan, melibatkan pemangku kepentingan, dan mengatasi permasalahan terkait perpindahan pekerjaan.	Program pelatihan transformasi digital Angkatan Darat A.S (Brones et al., 2021); kepemimpinan dan komunikasi (Inakefe et al., 2023).

Pemantauan dan evaluasi	Menetapkan mekanisme untuk menetapkan metrik kinerja, melakukan evaluasi, dan mengumpulkan umpan balik pengguna untuk memastikan perbaikan dan penyempurnaan strategi secara berkelanjutan.	Evaluasi Defense Digital Service (DDS) di Departemen Pertahanan A.S (Abiodun et al., 2021); pemantauan kinerja (Yıldırım & Bostancı, 2021).
-------------------------	---	---

Sumber: diolah oleh Penulis, 2024

Tabel ini merangkum komponen-komponen utama yang diperlukan untuk mengembangkan kerangka strategis yang meningkatkan efisiensi operasional melalui E-Government di sektor pertahanan. Dengan menangani setiap komponen secara sistematis, organisasi pertahanan dapat menciptakan kerangka kerja yang kuat dan mudah disesuaikan yang mendukung keberhasilan implementasi inisiatif E-Government, yang pada akhirnya mengarah pada peningkatan kinerja dan kesiapan operasional.

#### **4. Simpulan**

Kondisi implementasi E-Government di sektor pertahanan saat ini menunjukkan adanya kemajuan signifikan dan tantangan yang terus berlanjut. Solusi digital yang ada telah meningkatkan efisiensi operasional, meningkatkan keamanan, dan memfasilitasi pengambilan keputusan dan koordinasi yang lebih baik. Namun, mengatasi tantangan yang terkait dengan implementasi dan integrasi sangat penting untuk memaksimalkan manfaat dari inisiatif E-Government. Seiring dengan terus berkembangnya teknologi, sektor pertahanan harus beradaptasi dan berinovasi untuk sepenuhnya memanfaatkan potensi transformasi digital.

Keberhasilan implementasi E-Government di sektor pertahanan dipengaruhi oleh serangkaian faktor penting, termasuk kesiapan teknologi, langkah-langkah keamanan siber, budaya organisasi, dukungan kebijakan, dan integrasi sistem. Mengatasi faktor-faktor ini secara efektif dapat mengarah pada peningkatan efisiensi operasional, peningkatan pengambilan keputusan, dan kinerja organisasi pertahanan secara keseluruhan yang lebih baik. Ketika sektor pertahanan terus merangkul transformasi digital, pemahaman dan pengelolaan faktor-faktor ini akan menjadi kunci untuk mewujudkan potensi penuh dari inisiatif E-Government.

Mengembangkan kerangka kerja strategis untuk meningkatkan efisiensi operasional melalui E-Government di sektor pertahanan melibatkan pendekatan multifaset yang mencakup penilaian dan perencanaan, tata kelola dan pengembangan kebijakan, integrasi infrastruktur dan teknologi, keamanan siber dan manajemen risiko, pelatihan dan manajemen perubahan, serta pemantauan dan evaluasi. Dengan memanfaatkan wawasan dari implementasi yang berhasil dan mengatasi tantangan yang teridentifikasi, organisasi pertahanan dapat menciptakan kerangka kerja yang kuat yang memaksimalkan manfaat E-Government dan meningkatkan efisiensi operasional secara keseluruhan.

Berdasarkan kesimpulan, beberapa rekomendasi dapat diajukan untuk meningkatkan implementasi E-Government di sektor pertahanan. Pertama, perlu dilakukan penilaian mendalam terkait kesiapan teknologi dan perencanaan yang matang guna memastikan bahwa sistem yang diadopsi sesuai dengan kebutuhan operasional pertahanan. Kedua, tata kelola yang kuat serta kebijakan yang mendukung perlu dikembangkan untuk mendorong integrasi E-Government dengan proses pertahanan yang ada. Ketiga, meningkatkan keamanan siber melalui langkah-langkah yang lebih canggih dan manajemen risiko yang ketat sangat penting dalam menjaga kerahasiaan informasi dan keandalan sistem. Keempat, program pelatihan berkelanjutan dan manajemen perubahan harus diterapkan untuk memastikan personel pertahanan memiliki keterampilan yang diperlukan dalam mengoperasikan teknologi digital baru. Terakhir, pemantauan dan evaluasi secara teratur harus dilakukan untuk menilai keberhasilan implementasi dan mengidentifikasi area yang memerlukan perbaikan, guna terus meningkatkan efisiensi operasional di sektor pertahanan.

## Daftar Pustaka

- Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhalaf, R. S., & Arshad, H. (2021). A review on the security of the internet of things: Challenges and solutions. *Wireless Personal Communications, 119*, 2603–2637.
- Abusamhadana, G. A. O., Bakon, K. A., & Elias, N. F. (2021). E-government in Ghana: the benefits and challenges. *Abusamhadana, GAO, Bakon KA, & Elias NF (2021) "E-Government in Ghana: The Benefits and Challenges." Asia-Pacific Journal of Information Technology and Multimedia, 10(1)*, 124–140.
- Accenture. (2021). *Digital Defense: Strategies for E-Government in the Defense Sector*.
- Almamy, A. S. M. (2022). Understanding factors affecting e-government adoption in Saudi Arabia: the role of religiosity. *International Journal of Customer Relationship Marketing and Management (IJCRMM), 13(1)*, 1–15.
- Antoni, S., Rahayu, S., Yudi, Y., & Herawaty, N. (2024). Electronic Government and Accountability: Systematic Literature Review, Framework, and Agenda for Future Research. *Journal of Applied Business, Taxation and Economics Research, 3(6)*, 728–738.
- Brillianty, R. J. (2023). Analisis Perbandingan Politik, Ekonomi, Teknologi, Pertahanan Dan Keamanan Dan Sistem Pemerintahan 2 Negara Indonesia Dan Singapura. *Irpia: Jurnal Ilmiah Riset Dan Pengembangan*, 1–15.
- Brones, F., Zancul, E., & Carvalho, M. M. (2021). Insider action research towards companywide sustainable product innovation: ecodesign transition framework. *International Journal of Managing Projects in Business, 14(1)*, 150–178.
- Cahyani, N.P.K. and Putra, I.P.A.P. (2024) 'Governance And Digital Transformation: Analisis Ruang Kerja Virtual Melalui Perspektif E-Government Pada Pemerintahan Provinsi Bali', *Public Sphere Review, 3(1)*, pp. 1–11. Available at: <https://doi.org/10.30649/psr.v3i1.123>.
- Chivukula, R., Lakshmi, T. J., Kandula, L. R. R., & Alla, K. (2021). A study of cyber security issues and challenges. *2021 IEEE Bombay Section Signature Conference (IBSSC)*, 1–5.
- Chu, Y., & Xu, L. (2024). Research on Influencing Factors of Catch-Up in Complex Product Systems: Taking the China Manned Space Engineering Application System as an Example. *Systems, 12(10)*, 384.
- Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.
- Dawson, G. M. (2023). *An analysis of the legal frameworks that apply to the environmental remediation of sea-dumped chemical weapons*.
- Deloitte. (2021). *Governance in Digital Defense: A Strategic Approach*.
- DoD. (2022). *Defense Enterprise Resource Planning (DERP) System Overview*.
- Draheim, D., Krimmer, R., & Tammet, T. (2021). On state-level architecture of digital government ecosystems: From ICT-driven to data-centric. In *Transactions on Large-Scale Data-and Knowledge-Centered Systems XLVIII: Special Issue In Memory of Univ. Prof. Dr. Roland Wagner* (pp. 165–195). Springer.
- Firman, F., Sahrul, S., & Ramadoan, S. (2023). Analysis of efforts in the development of local government: e-government and public service management. *Jurnal Studi Ilmu Pemerintahan, 4(2)*, 25–36.
- Huang, J., Beling, P., Freeman, L., & Zeng, Y. (2022). Trustworthy AI for digital engineering transformation. In *Journal of Integrated Design and Process Science* (Vol. 25, Issue 1, pp. 1–7). SAGE Publications Sage UK: London, England.
- Inakefe, G. I., Basse, V. U., Ikeanyibe, O. M., Nwagboso, C. I., Agbor, U. I., Ebegbulem, J., Mbonu, F. I., & Ike, G. U. (2023). Digital Literacy and E-Governance Adoption for Service Delivery in Cross River State Civil Service. *International Journal of Electronic Government Research (IJEGR), 19(1)*, 1–23.

- Kim, C., & Kim, K. (2021). The institutional change from E-Government toward Smarter City; comparative analysis between royal borough of Greenwich, UK, and Seongdong-gu, South Korea. *Journal of Open Innovation: Technology, Market, and Complexity*, 7(1), 42.
- Kim, J.-S., Kim, K.-W., & Park, S.-S. (2023). The Impact of Leadership and Dynamic Capabilities on Firm Performance, Mediated by Digital Transformation-Aerospace & Defense Industry. *Journal of the Korean Society for Aviation and Aeronautics*, 31(3), 133–141.
- KPMG. (2022). *Cybersecurity in Defense: Protecting Digital Frontiers*.
- Kuhlmann, S., & Marienfeldt, J. (2023). Comparing local government systems and reforms in Europe: from New Public Management to Digital Era Governance? In *Handbook on Local and Regional Governance* (pp. 313–329). Edward Elgar Publishing.
- Liu, X. (2022). The study on national security in big data era. *Frontiers in Business, Economics and Management*, 5(3), 191–200.
- Lněnička, M., & Máchová, R. (2022). A theoretical framework to evaluate ICT disparities and digital divides: Challenges and implications for e-government development. *Review of Economic Perspectives*, 22(1), 25–51.
- Malodia, S., Dhir, A., Mishra, M., & Bhatti, Z. A. (2021). Future of e-Government: An integrated conceptual framework. *Technological Forecasting and Social Change*, 173, 121102.
- Manoharan, A. P., Ingrams, A., Kang, D., & Zhao, H. (2021). Globalization and worldwide best practices in E-Government. *International Journal of Public Administration*, 44(6), 465–476.
- NATO. (2022). *E-Government in Defense: Challenges and Opportunities*.
- NATO. (2023). *NATO Support and Procurement Agency: Automated Logistics Management*.
- NATO REVIEW. (2021, May 20). *Countering cognitive warfare: awareness and resilience*. NATO REVIEW. <https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html>
- Nwobodo, L. K., Nwaimo, C. S., & Adegbola, A. E. (2024). Enhancing cybersecurity protocols in the era of big data and advanced analytics. *GSC Advanced Research and Reviews*, 19(3), 203–214.
- OECD. (2021). *Digital Government Review of Estonia: Advancing Digital Transformation*.
- Pickering, J. C., & Fox, A. M. (2022). Enabling collaboration and communication across law enforcement jurisdictions: Data sharing in a multiagency partnership. *Criminal Justice Policy Review*, 33(7), 732–755.
- Saleh, S., Nakshabandi, O. A., Zeebaree, M., Ismael, G. Y., & Aqel, M. (2021). Organizational barriers which are facing electronic government implementation: The electronic government implementation framework. *Studies of Applied Economics*, 39(7).
- Sarjito, A. (2024). Enhancing National Security: Strategic Policy Development in Defense Management. *Jurnal Pelita Nusantara*, 2(1), 56–68.
- Sreedevi, A. G., Harshitha, T. N., Sugumaran, V., & Shankar, P. (2022). Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review. *Information Processing & Management*, 59(2), 102888.
- Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry*, 13(4), 597.
- Taliaferro, A. C., Gonzalez, L. M., Tillman, M., Ghosh, P., Clarke, P., & Hinkle, W. (2022). *Defense Governance and Management: Improving the Defense Management Capabilities of Foreign Defense Institutions A Guide to Capability-Based Planning (CBP)*. Institute for Defense Analyses.
- Tóth, A. (2023). *Information security threats in the digitalization of governance and their impact on elements of the defense sector*.
- Turner, M., Kim, J., & Kwon, S.-H. (2022). The political economy of E-Government innovation and success in Korea. *Journal of Open Innovation: Technology, Market, and Complexity*, 8(3), 145.
- UNDP. (2021). *E-Government for Sustainable Development in the Defense Sector*.



- United Nations E-Government Survey. (2022). *United Nations E-Government Survey 2022: The Future of Digital Government*. UN.
- Viana, A. C. A. (2021). Digital transformation in public administration: from e-Government to digital government. *International Journal of Digital Law*, 1, 29–44.
- Vollmer, B. (2021). NATO's Mission-Critical space capabilities under threat: cybersecurity gaps in the military space asset supply chain. *ArXiv Preprint ArXiv:2102.09674*.
- Yang, L., Elisa, N., & Eliot, N. (2019). Privacy and security aspects of E-government in smart cities. In *Smart cities cybersecurity and privacy* (pp. 89–102). Elsevier.
- Yıldırım, S., & Bostancı, S. H. (2021). The efficiency of e-government portal management from a citizen perspective: evidences from Turkey. *World Journal of Science, Technology and Sustainable Development*, 18(3), 259–273.
- Zimmerman, P., Gilbert, T., & Salvatore, F. (2019). Digital engineering transformation across the Department of Defense. *The Journal of Defense Modeling and Simulation*, 16(4), 325–338.
- Υφαντής, Β. (2024). *Cutting-edge computational systems and emerging technologies applied to e-government and virtual environments*.