CoPAR
Contemporary
Public Administration Review

Department of Public Administration
Parahyangan Catholic University
Ciumbuleuit 94, Bandung 40141, Indonesia
copar@unpar.ac.id

Integrasi Teknologi Jakarta Smart City dengan Sistem Komando dan Kendali untuk Penguatan Pertahanan Negara

Aris Sarjito* & Agung Risdhianto
Jurusan Manajemen Pertahanan Universitas Pertahanan Republik Indonesia

Kata Kunci
Interoperabilitas; Jakarta Smart City; Keamanan Siber; Pertahanan Negara; Sistem C4ISR

Abstrak
Program Jakarta Smart City yang berlandaskan Peraturan Gubernur No. 306 Tahun 2016, memiliki potensi besar untuk mendukung implementasi sistem Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) sebagai upaya untuk memperkuat pertahanan negara. Dengan teknologi yang terintegrasi, Jakarta Smart City dapat menyediakan data *real-time* dari sektor transportasi, logistik, dan situasi darurat yang sangat relevan dalam pengambilan keputusan strategis. Penelitian ini bertujuan untuk mengeksplorasi potensi, mengidentifikasi tantangan, dan merumuskan strategi integrasi antara teknologi Jakarta Smart City dan sistem C4ISR. Metode penelitian yang digunakan adalah pendekatan kualitatif dengan analisis deskriptif berbasis data sekunder dari dokumen kebijakan, laporan resmi, dan literatur terkini. Temuan menunjukkan bahwa Jakarta Smart City dapat mendukung fungsi intelijen, komando, dan kendali melalui data *real-time* dan infrastruktur teknologi seperti CCTV berbasis AI dan sensor IoT. Namun, terdapat tantangan signifikan, termasuk kesenjangan teknologi antara sistem sipil dan militer, risiko keamanan data, serta kurangnya koordinasi lintas instansi. Penelitian ini menyimpulkan keberhasilan integrasi memerlukan peningkatan interoperabilitas teknologi, penguatan keamanan siber, dan pembaruan regulasi nasional untuk mendukung sinergi antara sektor sipil dan militer. Dengan langkah strategis ini, Jakarta Smart City dapat berperan sebagai elemen strategis dalam memperkuat pertahanan negara.

Keywords
C4ISR System; Cybersecurity; Interoperability; Jakarta Smart City; National Defense

Abstract
Jakarta Smart City, established under Governor Regulation No. 306 of 2016, holds significant potential to support the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) system in strengthening national defense. By leveraging integrated technologies, Jakarta Smart City provides real-time data from many sectors such as transportation, logistics, and emergency management, which are highly relevant for strategic decision-making. This study aims to explore the potential, identify challenges, and formulate integration strategies between Jakarta Smart City technology and the C4ISR system. The research employs a qualitative approach with descriptive analysis based on secondary data from policy documents, official reports, and recent literature. Findings reveal that Jakarta Smart City can enhance intelligence, command, and control functions through real-time data and technological infrastructure, such as AI-powered CCTV and IoT sensors. However, significant challenges remain, including technological gaps between civilian and military systems, data security risks, and insufficient cross-agency coordination. In conclusion, successful integration requires improved interoperability between systems, enhanced cybersecurity measures, and updated national regulations to support synergy between civilian and military technologies. With these strategic measures, Jakarta Smart City can serve as a critical asset in bolstering national defense capabilities.

Correspondence Author Email: arissarjito@gmail.com
Submitted on 06 January 2025; revisions on 11 February 2025; online publication on 26 February 2025
Contemporary Public Administration Review (CoPAR)
https://doi.org/10.26593/copar.v2i2.8943.143-169

1. Pendahuluan

Program Jakarta Smart City didirikan berdasarkan Peraturan Gubernur Nomor 306 Tahun 2016 untuk memanfaatkan teknologi dalam meningkatkan efisiensi pengelolaan perkotaan. Tujuan utamanya adalah mengoptimalkan pengelolaan transportasi, logistik, dan respon darurat, sekaligus menyediakan layanan publik yang lebih transparan dan terintegrasi. Dengan dukungan regulasi, Jakarta Smart City telah berkembang menjadi platform teknologi strategis yang mampu menghadirkan data kaya dan terkoordinasi, yang tidak hanya berguna untuk pelayanan publik tetapi juga untuk keamanan dan pertahanan negara (Made & Mahayani, 2024). Namun, penelitian lain mengkritisi banyak proyek *smart city* di negara berkembang mengalami keterbatasan dalam infrastruktur digital dan standar keamanan, yang dapat menghambat integrasi dengan sistem militer atau pertahanan (Batty, 2018).

Pada era modern ini, ancaman yang dihadapi oleh kota besar seperti Jakarta tidak lagi terbatas pada ancaman fisik, tetapi juga mencakup ancaman multidimensional seperti serangan siber, terorisme, dan bencana alam. Teknologi *smart city* memiliki potensi besar untuk berperan dalam menangani tantangan tersebut, terutama melalui integrasi dengan sistem Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR). Sistem ini dirancang untuk mendukung pengambilan keputusan berbasis data dalam operasi keamanan dan pertahanan (Houichi et al., 2024). Dengan memanfaatkan data yang dihasilkan oleh Jakarta Smart City, sistem C4ISR dapat meningkatkan efektivitas dan efisiensi operasi, termasuk dalam intelijen, pengawasan, dan pengintaian (Hanggara, 2021). Namun, beberapa studi menyebutkan bahwa efektivitas sistem ini sangat tergantung pada kemampuan pemerintah dalam mengelola dan melindungi data yang dihasilkan (König, 2021).

Sebagai ibu kota negara, Jakarta menghadapi tantangan unik seperti kemacetan lalu lintas, tingginya kepadatan penduduk, dan kerentanan serangan terhadap infrastruktur kritis. Kompleksitas ini membutuhkan pendekatan teknologi yang terintegrasi untuk mendukung pengambilan keputusan yang cepat dan akurat dalam merespons ancaman. Teknologi Jakarta Smart City, seperti sensor Internet of Things (IoT) dan analitik data besar, mampu memberikan wawasan berbasis data secara *real-time*, yang menjadi elemen penting dalam mendukung sistem komando dan kendali (Caňares, 2018). Penelitian sebelumnya menunjukkan bahwa penggunaan teknologi serupa di beberapa kota besar dunia, termasuk Seoul dan Singapura, telah terbukti efektif dalam meningkatkan respons terhadap situasi

darurat (Yang et al., 2021). Namun, beberapa penelitian menunjukkan bahwa keberhasilan implementasi IoT dalam *smart city* sering kali tergantung pada kesiapan regulasi dan dukungan infrastruktur yang merata (Belli et al., 2020).

Sistem C4ISR memberikan kerangka kerja yang mendukung kolaborasi antara elemen-elemen pertahanan dan keamanan. Dengan mengintegrasikan data dari Jakarta Smart City, seperti pergerakan transportasi atau informasi logistik, sistem ini dapat digunakan untuk mengoordinasikan operasi keamanan dan pertahanan secara lebih efisien (Hutomo et al., 2021). Penelitian dari Chen et al. (2020) menyoroti bahwa keberhasilan integrasi ini sangat bergantung pada tingkat interoperabilitas antara sistem sipil dan militer, yang sering kali memiliki standar teknologi berbeda. Sebagai contoh, data dari sistem pemantauan lalu lintas dapat dimanfaatkan untuk mengatur pergerakan pasukan atau evakuasi selama kondisi darurat (Ma et al., 2025).

Namun, integrasi antara teknologi Jakarta Smart City dan sistem C4ISR menghadapi berbagai tantangan. Salah satunya keamanan data yang dihasilkan oleh *smart city* sering kali bersifat sensitif dan strategis, sehingga perlu perlindungan dari ancaman kebocoran atau serangan siber (Kim et al., 2023). Penelitian tentang keamanan siber dalam *smart city* menyoroti bahwa penggunaan sistem *cloud* dan konektivitas IoT yang tinggi dapat meningkatkan risiko serangan terhadap infrastruktur kritis (Perera et al., 2015). Selain itu, koordinasi antara instansi pemerintah daerah, militer, dan penyedia teknologi memerlukan kebijakan yang jelas dan dukungan infrastruktur yang kompatibel (Panda, 2023). Studi dari negara maju menunjukkan bahwa kegagalan dalam menetapkan regulasi yang ketat dapat menyebabkan penyalahgunaan data oleh pihak yang tidak berwenang (Zhang et al., 2021). Tantangan ini menjadi lebih kompleks karena terdapat perbedaan kebutuhan dan prioritas antara sektor sipil dan militer.

Untuk mengatasi tantangan tersebut, dibutuhkan pendekatan holistik yang mencakup peningkatan keamanan siber, pengembangan sistem yang interoperabel, dan pelatihan bagi personel yang terlibat. Selain itu, revisi terhadap Peraturan Gubernur Nomor 306 Tahun 2016 perlu dilakukan untuk mendukung integrasi teknologi sipil dan militer dalam program Jakarta Smart City (Izzuddin, 2022). Penelitian tentang kebijakan *smart city* di negara lain menunjukkan bahwa revisi regulasi yang fleksibel dapat mempercepat proses adopsi teknologi dalam sektor pertahanan (Keenan et al., 2024). Studi dari negara-negara maju seperti Korea Selatan menunjukkan bahwa integrasi yang efektif antara teknologi *smart city* dan sistem pertahanan dapat meningkatkan ketahanan nasional secara signifikan (Keenan et al., 2024).

Integrasi teknologi Jakarta Smart City dengan sistem komando dan kendali seperti C4ISR juga sejalan dengan agenda transformasi digital nasional yang dicanangkan oleh pemerintah. Program ini bertujuan untuk memperkuat ketahanan digital Indonesia dalam menghadapi tantangan global yang semakin kompleks, termasuk di bidang pertahanan (Wisnubroto, 2024; Lebang et al., 2023). Dengan memanfaatkan teknologi ini, Jakarta dapat menjadi model bagi kota-kota lain di Indonesia dalam membangun sistem pertahanan berbasis teknologi. Namun, beberapa studi menyebutkan bahwa transformasi digital yang efektif harus diimbangi dengan kesiapan infrastruktur dan sumber daya manusia yang memadai (West, 2018).

Secara keseluruhan, integrasi antara teknologi Jakarta Smart City dan sistem komando dan kendali adalah langkah strategis yang penting untuk memperkuat pertahanan negara. Tidak hanya mendukung respons yang lebih cepat terhadap ancaman, tetapi juga berkontribusi pada efisiensi operasional dan pengelolaan sumber daya yang lebih baik. Namun, untuk mencapai integrasi yang optimal, diperlukan regulasi yang lebih adaptif, sistem keamanan yang lebih tangguh, serta koordinasi lintas sektor yang kuat. Jika semua tantangan ini dapat diatasi, Jakarta dapat menjadi contoh sukses dalam memanfaatkan teknologi *smart city* sebagai bagian dari strategi pertahanan modern.

Jakarta Smart City diatur dalam Peraturan Gubernur No. 306 Tahun 2016, dikembangkan sebagai solusi berbasis teknologi yang menawarkan potensi besar untuk mendukung keamanan dan pertahanan negara. Di sisi lain, sistem C4ISR merupakan kerangka kerja strategis yang memungkinkan operasi pertahanan dilakukan secara efektif dengan memanfaatkan informasi yang akurat dan *real-time*. Integrasi data dan teknologi dari Jakarta Smart City dengan sistem C4ISR dapat memberikan keunggulan strategis, seperti pengambilan keputusan yang lebih cepat dan respons yang lebih efisien terhadap ancaman. Namun, proses integrasi ini menghadapi tantangan signifikan, termasuk perlindungan data sensitif, kesenjangan teknologi, koordinasi antarinstansi, dan kompatibilitas teknologi. Dengan meningkatnya kebutuhan akan strategi pertahanan yang modern dan efisien, penelitian ini berupaya mengkaji bagaimana Jakarta Smart City dapat dioptimalkan untuk mendukung sistem pertahanan negara melalui integrasi C4ISR.

Meskipun konsep *smart city* telah banyak diterapkan di berbagai kota besar untuk meningkatkan efisiensi layanan publik dan tata kelola kota, masih terdapat kesenjangan dalam penelitian terkait pemanfaatannya dalam sistem pertahanan dan keamanan berbasis C4ISR. Sebagian besar kajian saat ini lebih menitikberatkan pada aspek manajemen *smart city*, tanpa mengkaji secara mendalam bagaimana

teknologi ini dapat berkontribusi dalam kesadaran situasional (*situational awareness*), pengambilan keputusan berbasis data, serta interoperabilitas antar sistem militer dan sipil. Penelitian ini berusaha menjembatani kesenjangan tersebut dengan mengidentifikasi tantangan teknis seperti integrasi infrastruktur digital, keamanan siber, serta kompatibilitas sistem antara teknologi sipil dan militer. Selain itu, penelitian ini juga akan mengembangkan kerangka kerja yang dapat menjadi acuan bagi pemerintah dan pemangku kepentingan dalam menerapkan teknologi Jakarta Smart City secara efektif.

2. Tinjauan Pustaka

Dasar Hukum Jakarta Smart City

Program Jakarta Smart City didirikan berdasarkan Peraturan Gubernur Nomor 306 Tahun 2016, yang menjadi landasan hukum dalam pengelolaan teknologi untuk mendukung berbagai kebutuhan kota. Regulasi ini dirancang untuk memanfaatkan teknologi secara maksimal dalam meningkatkan efisiensi layanan publik, seperti pengelolaan transportasi, logistik, hingga respon darurat. Selain itu, peraturan ini juga mencerminkan visi modernisasi Jakarta sebagai kota cerdas yang tanggap terhadap tantangan perkotaan, baik dari aspek sosial, ekonomi, maupun keamanan (Made & Mahayani, 2024).

Namun, dalam konteks pertahanan negara, dasar hukum ini memiliki potensi yang belum sepenuhnya dimanfaatkan. Penelitian menunjukkan bahwa kebijakan yang mendukung pengelolaan data berbasis teknologi dapat menjadi elemen penting dalam memperkuat sistem pertahanan, terutama melalui integrasi dengan sistem C4ISR (Hutomo et al., 2021). Sebagai sistem strategis, C4ISR membutuhkan data yang akurat dan *real-time*, yang sebagian besar dapat disediakan oleh infrastruktur teknologi Jakarta Smart City. Meski demikian, implementasi regulasi ini perlu diperkuat dengan penyesuaian kebijakan yang lebih terarah pada kebutuhan pertahanan negara (Rifaid et al., 2023).

Beberapa kota seperti Singapura dan Seoul telah berhasil memanfaatkan teknologi *smart city* untuk mendukung sistem pertahanan mereka. Studi kasus dari kota-kota tersebut menunjukkan bahwa kerangka hukum yang mendukung sinergi antara teknologi sipil dan militer menjadi faktor kunci keberhasilan (Choi et al., 2020). Jakarta dapat belajar dari pengalaman ini, terutama dalam memastikan bahwa regulasi yang ada mendukung integrasi yang efektif antara teknologi *smart city* dan sistem pertahanan. Hal ini termasuk penguatan aspek keamanan data, yang menjadi salah satu tantangan utama dalam pengelolaan teknologi modern (Kim et al., 2023).

Dengan demikian, Peraturan Gubernur Nomor 306 Tahun 2016 adalah langkah awal yang strategis, namun memerlukan revisi untuk lebih relevan dalam konteks pertahanan negara. Penyesuaian ini perlu mencakup aspek interoperabilitas sistem, perlindungan data sensitif, dan harmonisasi kebijakan antara pemerintah daerah dan nasional (Ma et al., 2025). Langkah ini akan memastikan bahwa Jakarta Smart City tidak hanya menjadi solusi untuk tata kelola kota, tetapi juga menjadi elemen penting dalam mendukung keamanan dan pertahanan negara.

Konsep Teknologi Smart City

Teknologi *smart city* adalah penerapan teknologi informasi dan komunikasi yang terintegrasi untuk meningkatkan efisiensi, keberlanjutan, dan kualitas hidup di kawasan perkotaan. Konsep ini melibatkan elemen utama seperti IoT, *big data*, dan data analitik, yang bekerja bersama untuk menciptakan sistem kota yang mampu memantau, mengelola, dan mengoptimalkan berbagai layanan secara *real-time*. IoT memungkinkan pengumpulan data melalui sensor yang tersebar di berbagai infrastruktur kota, seperti jalan, jaringan listrik, dan fasilitas publik. Sementara itu, *big data* dan data analitik membantu memproses dan menganalisis data dalam skala besar untuk mendukung pengambilan keputusan berbasis informasi (Made & Mahayani, 2024).

Dalam konteks tata kelola perkotaan, teknologi *smart city* telah memainkan peran penting menyelesaikan tantangan sehari-hari. Misalnya, teknologi ini digunakan untuk mengurangi kemacetan lalu lintas, mengoptimalkan penggunaan energi, dan memberikan respons yang lebih cepat dalam situasi darurat. Namun, manfaatnya tidak hanya terbatas pada pengelolaan kota. Data *real-time* yang dihasilkan dari infrastruktur kota dapat dimanfaatkan untuk mendeteksi ancaman keamanan, seperti aktivitas kriminal atau ancaman siber, dan mendukung sistem pertahanan negara yang lebih tangguh (Hutomo et al., 2021).

Teknologi *smart city* juga memberikan peluang untuk meningkatkan koordinasi antarinstansi melalui platform digital yang terintegrasi. Teknologi ini tidak hanya menyelesaikan masalah perkotaan tetapi juga memperkuat sistem keamanan dan pertahanan negara (Ma et al., 2025). Oleh karena itu, teknologi *smart city* adalah aset penting yang mampu mendukung keberlanjutan kota sekaligus menjadi komponen strategis untuk pertahanan negara di era modern.

Sistem C4ISR dalam Pertahanan

Sistem C4ISR memainkan peran penting dalam operasi pertahanan modern. Sistem ini dirancang untuk mengintegrasikan berbagai elemen, seperti pengumpulan informasi, analitik data, dan pengambilan keputusan berbasis data

(Sarjito, 2023). Salah satu fungsi utamanya adalah menyediakan intelijen *real-time* dari berbagai sumber, seperti sensor di lapangan, satelit, atau *drone*. Data ini dianalisis untuk memberikan wawasan strategis yang membantu pengambilan keputusan dengan cepat dan tepat, terutama dalam situasi kritis. Selain itu, C4ISR memungkinkan komunikasi yang aman dan terkoordinasi antarunit militer, memastikan bahwa operasi dapat berjalan efisien dan terkendali (Hutomo et al., 2021).

Penggunaan C4ISR telah diterapkan secara luas di banyak negara dan memberikan hasil yang signifikan. Di Amerika Serikat, sistem ini digunakan dalam operasi militer di Timur Tengah untuk meningkatkan kemampuan pengawasan dan koordinasi pasukan, yang berkontribusi pada keberhasilan banyak misi strategis (Kendzierskyj & Jahankhani, 2020). Di Korea Selatan, C4ISR diintegrasikan dengan teknologi Smart City untuk memantau wilayah perbatasan serta mendeteksi ancaman keamanan siber, menjadikannya alat yang tangguh dalam merespons ancaman keamanan nasional (Ng, 2022; Yang et al., 2021). Sementara itu, Singapura menggunakan sistem ini untuk memperkuat pengawasan maritim di wilayah strategis, membantu mencegah aktivitas ilegal seperti penyelundupan dan perompakan (Tikanmäki et al., 2021).

Implementasi C4ISR bukan tanpa tantangan. Infrastruktur teknologi yang diperlukan untuk mendukung sistem ini harus canggih dan mampu beroperasi lintas platform. Selain itu, keamanan data menjadi perhatian utama, terutama ketika sistem ini digunakan untuk operasi yang melibatkan informasi sensitif. Di India, pengembangan C4ISR berbasis satelit domestik menunjukkan potensi besar dalam meningkatkan kemampuan pertahanan udara, tetapi juga menyoroti perlunya investasi besar dalam keamanan data dan interoperabilitas sistem (Bommakanti, 2020). Studi kasus dari negara-negara ini menegaskan bahwa keberhasilan implementasi C4ISR sangat bergantung pada dukungan kebijakan yang kuat, teknologi yang andal, serta pelatihan personel yang berkesinambungan (Ma et al., 2025).

Di Indonesia, integrasi serupa masih menghadapi tantangan yang mencakup kurangnya koordinasi antarinstansi, kesiapan teknologi, dan perlunya regulasi yang lebih mendukung. Jika tantangan ini dapat diatasi, integrasi teknologi *smart city* dan C4ISR akan memperkuat pertahanan nasional secara signifikan, menjadikannya sistem yang tidak hanya melindungi wilayah, tetapi juga mengoptimalkan sumber daya nasional secara lebih efektif.

3. Metode

Penelitian ini menggunakan pendekatan kualitatif dengan analisis deskriptif-eksploratif. Pendekatan ini bertujuan untuk memahami secara mendalam potensi dan tantangan integrasi teknologi Jakarta Smart City dengan sistem C4ISR. Menurut Creswell (2018), penelitian kualitatif sangat cocok untuk mengeksplorasi fenomena kompleks dan mendalam, terutama dalam konteks sosial, teknologi, dan kebijakan. Dengan pendekatan ini, penelitian berupaya mengeksplorasi pola, hubungan, dan wawasan strategis terkait integrasi teknologi yang mendukung pertahanan negara.

Penelitian ini menggunakan data sekunder yang menurut Creswell (2018), adalah data yang dikumpulkan dari sumber yang telah tersedia, seperti dokumen, laporan, dan literatur terkait. Data yang dianalisis meliputi: (1) Peraturan Gubernur No. 306 Tahun 2016, yang menjadi dasar hukum pengelolaan Jakarta Smart City (Diskominfo, 2016); (2) Laporan resmi dari Jakarta Smart City yang membahas implementasi teknologi, kebijakan, dan infrastrukturnya; (3) Literatur akademik tentang teknologi C4ISR, termasuk studi kasus dari negara lain terkait implementasi dan integrasinya dengan sistem sipil; (4) Standar keamanan dan interoperabilitas internasional, seperti ISO/IEC 27001 untuk keamanan informasi serta ISO/IEC 30182 terkait arsitektur data untuk *smart city* (International Organization for Standardization, 2020); dan (5) Sertifikasi dan regulasi teknis yang berlaku, termasuk NIST SP 800-53 yang digunakan dalam sistem keamanan C4ISR serta ISO 22301 yang berkaitan dengan manajemen keberlanjutan layanan kritis dalam infrastruktur perkotaan (NIST, 2021).

Pengumpulan data dilakukan dengan meninjau dokumen-dokumen publik, artikel jurnal, dan buku yang diterbitkan dalam lima tahun terakhir. Fokus utama adalah menemukan informasi yang relevan untuk menjelaskan hubungan antara regulasi Jakarta Smart City, teknologi, dan kebutuhan strategis pertahanan negara (Hutomo et al., 2021; Yang et al., 2021). Penelitian ini juga mengacu pada *framework* keamanan siber militer yang telah diterapkan di beberapa negara, seperti Cybersecurity Maturity Model Certification (CMMC) dari Departemen Pertahanan Amerika Serikat dan Kerangka Keamanan Siber European Union Agency for Cybersecurity (ENISA) dari Uni Eropa (Department of Defense, 2024; ENISA, 2021).

Penelitian ini juga meninjau protokol komunikasi dan enkripsi data dalam sistem *smart city* dan C4ISR, seperti Advanced Encryption Standard (AES-256), Transport Layer Security (TLS) 1.3, dan IPsec (Internet Protocol Security), yang umum digunakan dalam infrastruktur teknologi pertahanan (Kim et al., 2023). Metode pengumpulan data ini bertujuan untuk memastikan bahwa analisis yang dilakukan tidak hanya mempertimbangkan aspek kebijakan, tetapi juga

memperhitungkan standar teknis yang diperlukan untuk mengintegrasikan teknologi Jakarta Smart City dengan sistem C4ISR secara aman dan efektif.

Analisis data dilakukan menggunakan metode analisis tematik, yang menurut Creswell (2018), sangat efektif untuk mengidentifikasi tema-tema kunci dari data tekstual. Dalam penelitian ini, analisis tematik digunakan untuk mengidentifikasi pola-pola yang berkaitan dengan peluang, tantangan, dan strategi integrasi antara Jakarta Smart City dan sistem C4ISR. Proses analisis mencakup pengkodean data, penemuan tema-tema utama, dan penyusunan rekomendasi berdasarkan temuan (Nowell et al., 2017). Melalui metode ini, penelitian diharapkan dapat memberikan wawasan yang lebih mendalam mengenai bagaimana regulasi dan teknologi dapat diselaraskan untuk mendukung kebutuhan strategis pertahanan negara. Pendekatan ini memungkinkan peneliti tidak hanya memahami fenomena secara menyeluruh, tetapi juga memberikan solusi praktis yang relevan (Kim et al., 2023).

4. Hasil

Penelitian ini menunjukkan bahwa Jakarta Smart City memiliki potensi besar untuk mendukung sistem C4ISR, terutama dalam meningkatkan kesadaran situasional dan pengambilan keputusan berbasis data dalam operasi pertahanan. Data *real-time* yang dihasilkan dari sistem inidapat digunakan untuk mempercepat respons terhadap ancaman dan meningkatkan efisiensi operasional pertahanan nasional.

Tetapi, integrasi ini tidak semudah menyatukan dua teknologi yang berbeda. Perbedaan infrastruktur digital antara sistem sipil dan militer menjadi kendala interoperabilitas, di mana Jakarta Smart City menggunakan protokol komunikasi terbuka, sementara C4ISR beroperasi dengan standar keamanan tinggi dan jaringan tertutup. Selain itu, keamanan data menjadi isu krusial, karena sistem *smart city* yang terkoneksi luas lebih rentan terhadap serangan siber, yang bisa membahayakan informasi strategis pertahanan. Koordinasi antarinstansi juga menjadi tantangan, karena integrasi ini membutuhkan sinkronisasi antara pemerintah daerah, militer, dan sektor swasta yang selama ini bekerja dengan prioritas berbeda.

Untuk menjawab tantangan ini, penelitian ini merekomendasikan beberapa strategi, seperti mengembangkan standar komunikasi yang kompatibel antara sistem sipil dan militer, mengadopsi sistem keamanan siber berbasis Zero Trust Architecture (ZTA) dan enkripsi AES-256, serta menerapkan kebijakan perlindungan data yang lebih ketat. Dari sisi regulasi, revisi terhadap Peraturan Gubernur No. 306 Tahun 2016 menjadi langkah penting agar Jakarta Smart City

tidak hanya berfokus pada layanan publik, tetapi juga mendukung ketahanan nasional.

Temuan ini mengisi kesenjangan dalam kajian sebelumnya, yang lebih banyak berfokus pada pengelolaan *smart city* tanpa melihat potensinya dalam sistem pertahanan. Dengan kerangka kerja yang telah dikembangkan dalam penelitian ini, Jakarta Smart City dapat menjadi model integrasi teknologi sipil dan militer yang lebih efektif, aman, dan berkelanjutan. Jika diterapkan dengan baik, Jakarta tidak hanya akan menjadi kota cerdas yang efisien, tetapi juga komponen strategis dalam pertahanan nasional yang siap menghadapi tantangan di era digital. Tabel 1 adalah ringkasan temuan utama penelitian ini:

Tabel 1. Temuan Penelitian dan Strategi Integrasi Jakarta Smart City

Kategori	Temuan
Potensi Jakarta Smart City dalam C4ISR	Jakarta Smart City memiliki potensi besar dalam mendukung sistem C4ISR dengan menyediakan data *real-time* yang dapat digunakan untuk meningkatkan kesadaran situasional dan pengambilan keputusan berbasis data dalam operasi pertahanan.
Manfaat Data *Real-Time* dalam Pertahanan	Data *real-time* dari pemantauan lalu lintas, logistik, dan deteksi dini keadaan darurat dapat mempercepat respons terhadap ancaman dan meningkatkan efisiensi operasional dalam pertahanan nasional.
Tantangan Integrasi: Infrastruktur Digital	Jakarta Smart City menggunakan protokol komunikasi terbuka, sedangkan sistem C4ISR memiliki standar keamanan tinggi dan jaringan tertutup, sehingga menciptakan kesenjangan interoperabilitas.
Tantangan Integrasi: Keamanan Data	Sistem *smart city* yang terkoneksi luas lebih rentan terhadap serangan siber, yang berpotensi membahayakan informasi strategis pertahanan.
Tantangan Integrasi: Koordinasi Antarinstansi	Integrasi ini membutuhkan sinkronisasi antara pemerintah daerah, militer, dan sektor swasta, yang memiliki perbedaan prioritas dan sistem kerja.

Strategi Integrasi: Standar Komunikasi	Diperlukan pengembangan standar komunikasi yang kompatibel antara sistem sipil dan militer untuk mengatasi hambatan interoperabilitas.
Strategi Integrasi: Keamanan Siber	Penerapan sistem keamanan siber berbasis ZTA dan enkripsi AES-256 dapat meningkatkan perlindungan data terhadap ancaman siber.
Strategi Integrasi: Kebijakan & Regulasi	Revisi terhadap Peraturan Gubernur No. 306 Tahun 2016 diperlukan agar Jakarta Smart City tidak hanya berfokus pada layanan publik tetapi juga mendukung ketahanan nasional.
Implikasi & Kesimpulan	Jakarta Smart City dapat menjadi model integrasi teknologi sipil dan militer yang efektif, aman, dan berkelanjutan, yang berkontribusi pada ketahanan nasional di era digital.

Sumber: Hasil Penelitian Penulis

Jika tantangan utama dapat diatasi, Jakarta Smart City bisa menjadi model integrasi teknologi sipil dan militer yang efektif dan aman. Ini bukan hanya tentang menciptakan kota yang lebih cerdas, tetapi juga membangun ekosistem pertahanan yang lebih kuat dan adaptif di era digital. Dengan langkah-langkah yang tepat, Jakarta bisa menjadi contoh sukses *smart city* yang mendukung ketahanan nasional.

5. Pembahasan

Potensi Jakarta Smart City dalam Mendukung C4ISR

Jakarta Smart City memiliki potensi besar dalam mendukung sistem C4ISR. Dengan teknologi yang terintegrasi, sistem ini bisa menyediakan data *real-time* dari berbagai sektor, seperti transportasi, logistik, hingga manajemen situasi darurat. Ketersediaan data ini berperan dalam mempercepat pengambilan keputusan strategis untuk operasi pertahanan negara. Sebagai pusat inovasi teknologi perkotaan, Jakarta Smart City menawarkan peluang besar untuk diintegrasikan dengan sistem pertahanan guna menghadapi ancaman keamanan modern (Hutomo et al., 2021).

Jakarta Smart City memiliki keunggulan dalam memantau pergerakan transportasi secara *real-time*. Data ini dapat dimanfaatkan oleh sistem C4ISR untuk mendukung logistik militer, misalnya dengan menentukan jalur transportasi paling aman dan efisien saat keadaan darurat. Contohnya, informasi lalu lintas

dapat digunakan untuk merancang jalur evakuasi tercepat atau mengoptimalkan pengiriman pasokan ke wilayah strategis (Susantono et al., 2024).

Penerapan sensor IoT dalam Jakarta Smart City dapat mendeteksi dini kondisi darurat, seperti banjir, kebakaran, atau kecelakaan lalu lintas. Data ini dapat dikirim langsung ke pusat komando, sehingga pengambil keputusan bisa merespon lebih cepat dalam operasi penyelamatan atau mitigasi bencana. Dengan demikian, integrasi ini meningkatkan adaptabilitas C4ISR dalam menghadapi berbagai ancaman yang muncul secara tiba-tiba (Sumari, 2014). Dari sisi logistik, data *real-time* dari sistem *smart city* dapat membantu dalam pengelolaan distribusi pasokan selama operasi militer. Dengan informasi yang akurat tentang rute pengiriman, titik kemacetan, atau potensi gangguan lainnya, sistem C4ISR bisa memastikan operasi logistik berjalan lancar dan sesuai dengan kebutuhan strategi pertahanan (Yang et al., 2021).

Seberapa Siap Infrastruktur Teknologi Jakarta Smart City?

Dari segi infrastruktur, Jakarta Smart City sudah cukup maju dengan berbagai sistem yang mendukung pengumpulan dan pengolahan data secara *real-time*. Beberapa teknologi utama yang sudah diterapkan mencakup: (1) Jaringan CCTV berbasis Kecerdasan Buatan (AI) dengan kemampuan pengenalan wajah; (2) Sistem pemantauan lalu lintas berbasis AI yang bisa menganalisis pola kemacetan dan mendeteksi anomali; dan (3) Sensor IoT di berbagai titik strategis kota yang bisa mengumpulkan data lingkungan, pergerakan kendaraan, serta kondisi infrastruktur. Teknologi ini tentu sangat berguna dalam mendukung kebutuhan intelijen dan pengawasan dalam sistem C4ISR (Kim et al., 2023).

Dalam pelaksanaannya, integrasi antara Jakarta Smart City dan sistem C4ISR menghadapi sejumlah tantangan. Salah satu kendala utama terkait kompatibilitas antara sistem sipil dan militer. Teknologi militer biasanya memiliki standar keamanan yang sangat ketat, sementara sistem *smart city* cenderung lebih fleksibel dan terbuka. Akibatnya, integrasi antara kedua sistem ini bisa menjadi sulit jika tidak ada standar komunikasi dan interoperabilitas yang jelas. Menurut Kendzierskyj & Jahankhani (2020), solusi dari masalah ini adalah mengembangkan protokol teknis yang bisa menjembatani kebutuhan kedua sistem tanpa mengorbankan keamanan informasi.

Keamanan data menjadi isu krusial dalam implementasi teknologi ini. Informasi yang dikumpulkan oleh Jakarta Smart City, seperti data infrastruktur strategis dan pergerakan logistik, berpotensi menjadi target serangan siber. Jika data tersebut jatuh ke pihak tidak berwenang, operasi militer dapat terganggu, bahkan menimbulkan ancaman terhadap keamanan nasional. Oleh karena itu,

penguatan sistem keamanan siber harus menjadi prioritas dalam memastikan kesiapan Jakarta Smart City untuk mendukung C4ISR (Bitzinger, 2021; Kulve & Smit, 2003).

Untuk mengatasi tantangan ini, Jakarta Smart City perlu mengadopsi beberapa standar keamanan informasi internasional, seperti: (1) ISO/IEC 27001 – Standar keamanan informasi untuk sistem *smart city*; (2) ISO/IEC 30182 – Standar interoperabilitas data untuk integrasi *smart city* dengan sistem lainnya; (3) NIST SP 800-53 – Framework keamanan siber yang sering digunakan dalam sistem militer (NIST, 2021); (4) CMMC, yang memastikan bahwa sistem dapat melindungi data sensitif dari ancaman siber (Department of Defense, 2024). Dengan menerapkan standar ini, Jakarta Smart City bisa memastikan bahwa sistemnya siap mendukung kebutuhan operasional pertahanan tanpa meningkatkan risiko serangan siber.

Relevansi Jakarta Smart City untuk Sistem C4ISR

Relevansi Jakarta Smart City dalam mendukung sistem C4ISR sangat jelas terlihat dari kemampuannya untuk mengintegrasikan berbagai data secara *real-time*. Dalam konteks operasi pertahanan, data ini bisa dimanfaatkan untuk: (1) komando dan kendali, memantau situasi di lapangan secara langsung; (2) intelijen dan pengawasan, mengumpulkan serta menganalisis data untuk mengidentifikasi potensi ancaman; dan (3) koordinasi unit militer, memastikan bahwa setiap unit bisa berkomunikasi dan bertindak secara efisien. Sebagai contoh, jaringan CCTV berbasis AI dari Jakarta Smart City bisa digunakan untuk mengidentifikasi individu mencurigakan atau melacak aktivitas yang berisiko tinggi (Tikanmäki et al., 2021).

Pengalaman dari negara lain menunjukkan bahwa integrasi teknologi *smart city* dengan C4ISR benar-benar bisa meningkatkan efektivitas pertahanan. Diperlukan investasi lebih lanjut dalam pengembangan infrastruktur dan pelatihan personel militer serta sipil. Pemerintah juga perlu memastikan bahwa regulasi yang ada, seperti Peraturan Gubernur No. 306 Tahun 2016, benar-benar mendukung integrasi teknologi ini secara komprehensif (Ma et al., 2025).

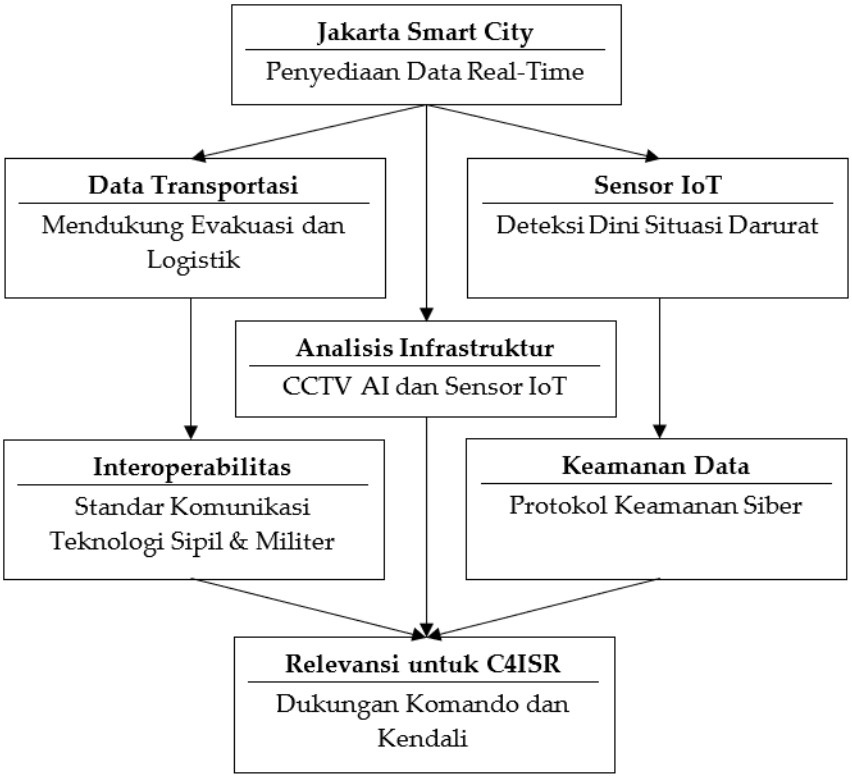
Keberhasilan integrasi Jakarta Smart City dengan sistem C4ISR bergantung pada beberapa faktor krusial. Pertama, standar keamanan data dan sistem siber harus ditingkatkan untuk melindungi informasi strategis dari ancaman siber, mengingat tingginya risiko kebocoran dan serangan digital. Kedua, diperlukan protokol komunikasi yang jelas antara sistem sipil dan militer agar kedua platform dapat saling berbagi data secara aman dan efisien tanpa mengorbankan standar operasional masing-masing. Ketiga, pelatihan personel harus diperkuat agar baik pihak militer maupun sipil mampu memanfaatkan data yang dihasilkan oleh

Jakarta Smart City dalam perencanaan dan eksekusi strategi pertahanan secara optimal. Jika semua tantangan ini dapat diatasi, Jakarta Smart City akan bertransformasi menjadi komponen strategis yang tidak hanya meningkatkan efisiensi tata kelola perkotaan, tetapi juga memperkuat keamanan nasional di era digital yang semakin kompleks.

Flowchart pada Gambar 1 menggambarkan bagaimana Jakarta Smart City menyediakan data dan mendukung sistem C4ISR, serta mengilustrasikan elemen-elemen utama dari potensi dan tantangannya. *Flowchart* ini menunjukkan alur utama potensi Jakarta Smart City, mulai dari penyediaan data *real-time*, analisis infrastruktur teknologi, hingga bagaimana data tersebut mendukung fungsi utama C4ISR, seperti komando, kendali, dan pengawasan. Diagram ini juga mengidentifikasi tantangan, seperti interoperabilitas teknologi sipil dan militer, serta keamanan data.

Jakarta Smart City memiliki peran strategis dalam mendukung pertahanan negara melalui integrasi dengan sistem C4ISR. Dengan menyediakan data *real-time* yang relevan dan didukung oleh infrastruktur teknologi canggih, sistem ini dapat membantu meningkatkan efektivitas operasional militer. Namun, untuk mewujudkan integrasi yang optimal, diperlukan langkah-langkah strategis, seperti meningkatkan interoperabilitas teknologi antara sektor sipil dan militer, memperkuat keamanan data, dan membangun kolaborasi lintas instansi. Jika tantangan ini dapat diatasi, Jakarta Smart City tidak hanya menjadi solusi inovatif untuk tata kelola perkotaan, tetapi juga elemen penting dalam memperkuat keamanan dan pertahanan negara.

Gambar 1. Potensi Jakarta Smart City dalam Mendukung C4ISR



Sumber: Disusun oleh penulis

Tantangan Integrasi

Meskipun Jakarta Smart City memiliki potensi besar untuk mendukung sistem C4ISR, tantangan dalam mengintegrasikan kedua sistem ini tetap signifikan. Tantangan tersebut mencakup kesenjangan teknologi, risiko keamanan data, dan koordinasi antarinstansi, yang semuanya membutuhkan solusi teknis yang komprehensif agar integrasi berjalan lancar dan efektif.

Kesenjangan antara teknologi Jakarta Smart City dan kebutuhan sistem C4ISR

Jakarta Smart City dirancang untuk kebutuhan sipil, seperti transportasi, logistik, dan manajemen darurat, sementara sistem C4ISR berfokus pada operasi militer yang membutuhkan kecepatan, keakuratan, dan keamanan tingkat tinggi. Perbedaan ini menciptakan kesenjangan antara teknologi sipil yang lebih terbuka dan sistem militer yang memiliki standar ketat dalam keamanan dan keandalan operasional. Menurut Hutomo et al. (2021), teknologi sipil sering kali tidak memenuhi standar keamanan dan operasional yang dibutuhkan dalam aplikasi militer, sehingga menyulitkan integrasi tanpa adanya modifikasi teknis yang signifikan.

Selain itu, protokol komunikasi dalam Jakarta Smart City cenderung menggunakan infrastruktur berbasis TCP/IP standar komersial, sementara sistem

C4ISR memanfaatkan jaringan komunikasi taktis berbasis protokol militer yang terenkripsi, seperti Link 16, Joint Tactical Radio System (JTRS), atau Mobile Ad Hoc Networks (MANETs) (Yang et al., 2021). Ketidaksesuaian protokol ini dapat menghambat interoperabilitas, yang merupakan elemen kunci dalam integrasi teknologi pertahanan. Untuk mengatasi masalah ini, diperlukan pengembangan gateway komunikasi atau middleware berbasis protokol standar militer seperti NATO STANAG 4586 dan MIL-STD-1553, yang memungkinkan sistem sipil dan militer bertukar data tanpa mengorbankan keamanan dan efisiensi jaringan.

Risiko keamanan data dan perlindungan informasi sensitif

Jakarta Smart City menghasilkan data strategis yang mencakup informasi pergerakan transportasi, lokasi infrastruktur penting, dan pola logistik. Jika data ini jatuh ke tangan yang salah, potensinya dapat dimanfaatkan untuk sabotase atau ancaman terhadap keamanan nasional (Kim et al., 2023). Salah satu risiko utama dalam sistem Jakarta Smart City adalah serangan siber melalui metode Man-in-the-Middle (MitM), Distributed Denial of Service (DDoS), dan Advanced Persistent Threats (APT), yang sering kali menargetkan jaringan terbuka dan kurang terlindungi dibandingkan infrastruktur militer (Jakarta Smart City, 2023).

Sistem enkripsi data dalam Jakarta Smart City masih menggunakan standar umum seperti AES-128 atau TLS 1.2, yang dalam konteks militer masih dianggap kurang kuat untuk menangkal serangan dari aktor siber tingkat tinggi. Sebaliknya, sistem C4ISR biasanya mengadopsi AES-256, Suite B Cryptography, serta Quantum-Resistant Encryption yang jauh lebih aman (NIST, 2021). Untuk mengurangi risiko ini, Jakarta Smart City perlu mengimplementasikan sistem keamanan yang lebih tangguh, seperti Intrusion Detection and Prevention Systems (IDPS), Security Information and Event Management (SIEM), serta ZTA. Selain itu, penggunaan teknologi *blockchain* untuk manajemen data sensitif juga dapat menjadi solusi dalam meningkatkan integritas dan ketertelusuran data (Bitzinger, 2021).

Koordinasi antarinstansi: menghubungkan pemerintah daerah dan militer

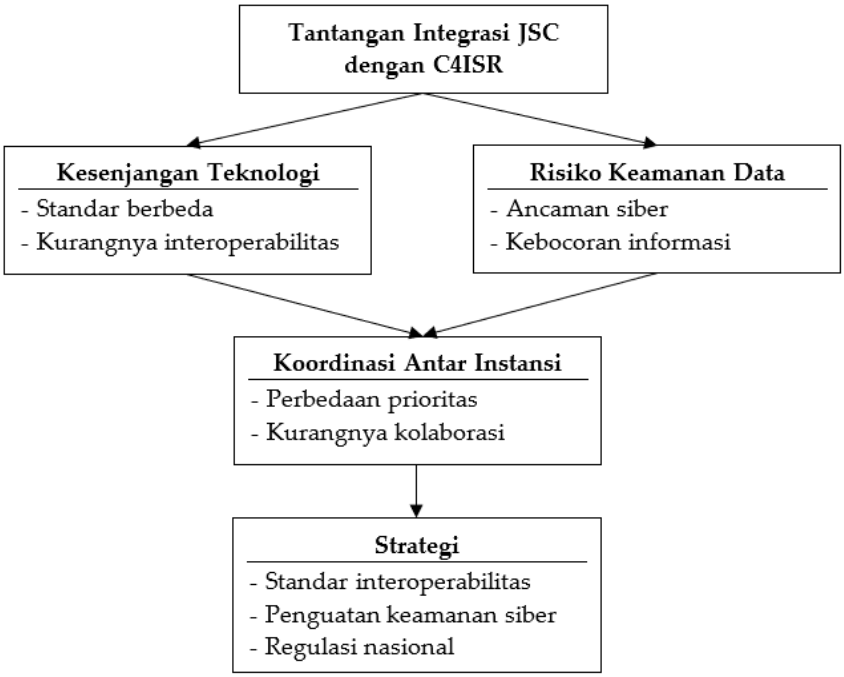
Kurangnya koordinasi antara pemerintah daerah, yang mengelola Jakarta Smart City, dan instansi militer, yang bertanggung jawab atas sistem C4ISR, menjadi tantangan besar dalam upaya integrasi ini. Kedua institusi memiliki struktur organisasi yang berbeda, serta prioritas yang tidak selalu selaras (Lintasarta, 2022; Seputar Birokrasi, 2024).Pemerintah daerah lebih berorientasi pada pelayanan publik dan efisiensi perkotaan, sementara militer lebih menitikberatkan pada keamanan nasional dan operasi strategis. Hal ini sering kali menyebabkan kesenjangan dalam komunikasi, pengambilan keputusan bersama,

serta pembagian tanggung jawab dalam pengelolaan data sensitif. Selain itu, regulasi yang ada, seperti Peraturan Gubernur No. 306 Tahun 2016, hanya berfokus pada tata kelola perkotaan dan belum mencakup aspek pertahanan negara, sehingga menciptakan kekosongan kebijakan yang dapat menghambat integrasi (Susantono et al., 2024).

Untuk mengatasi hambatan ini, diperlukan kerangka regulasi yang lebih adaptif dan memungkinkan adanya sinergi antara sektor sipil dan militer, seperti yang diterapkan di Korea Selatan. Negara tersebut telah mengadopsi regulasi nasional yang mengatur interoperabilitas antara teknologi *smart city* dan sistem pertahanan, yang memungkinkan sinkronisasi data dalam sistem keamanan siber nasional (Yang et al., 2021). Pendekatan serupa dapat diterapkan di Indonesia dengan membentuk satuan tugas khusus yang bertanggung jawab atas integrasi Jakarta Smart City dengan sistem pertahanan, sehingga koordinasi antara pemerintah daerah dan militer menjadi lebih efektif. Selain itu, pembangunan pusat data bersama yang memungkinkan akses terkontrol bagi kedua pihak akan memastikan bahwa informasi sensitif dapat digunakan secara optimal tanpa mengorbankan keamanan.

Untuk mendukung keberlanjutan sistem, model Public-Private Partnership (PPP) dengan perusahaan teknologi dapat diterapkan guna menghadirkan solusi inovatif, sekaligus memastikan bahwa sistem yang dikembangkan tetap aman, efisien, dan sesuai dengan standar pertahanan nasional. *Flowchart* di bawah ini memberikan ilustrasi visual tentang tantangan-tantangan utama yang dihadapi dan solusi yang direkomendasikan untuk mengatasi hambatan tersebut. Dari isu teknis hingga langkah strategis, seperti penguatan protokol keamanan, pengembangan standar interoperabilitas, dan pembaruan regulasi, semuanya terangkum dengan jelas.

Gambar 2. Tantangan dalam Integrasi Jakarta Smart City dengan C4ISR



Sumber: Disusun oleh penulis

Flowchart ini menggarisbawahi tiga tantangan utama yang perlu diatasi dalam mengintegrasikan Jakarta Smart City dengan sistem C4ISR: kesenjangan teknologi, risiko keamanan data, dan hambatan koordinasi lintas sektor. Tantangan ini memerlukan solusi yang terfokus, seperti pengembangan protokol teknis yang seragam untuk meningkatkan interoperabilitas, penguatan keamanan siber untuk melindungi data sensitif, dan regulasi nasional yang memastikan kolaborasi efektif antara sektor sipil dan militer.

Strategi Integrasi Jakarta Smart City dengan C4ISR

Integrasi antara teknologi Jakarta Smart City dan sistem C4ISR memerlukan strategi yang komprehensif dan mencakup berbagai aspek teknis serta organisasi. Strategi ini harus mencakup peningkatan interoperabilitas sistem, penguatan keamanan siber, membangun kolaborasi antara pengelola Jakarta Smart City dan instansi pertahanan, serta menyusun regulasi yang mendukung sinergi teknologi sipil dan militer. Pendekatan yang menyeluruh pada aspek ini menjadi kunci keberhasilan integrasi untuk menciptakan sistem pertahanan berbasis teknologi yang kuat dan responsif.

Teknologi: Meningkatkan Interoperabilitas Sistem Dan Keamanan Siber

Interoperabilitas menjadi tantangan utama dalam menghubungkan sistem Jakarta Smart City yang bersifat sipil dengan sistem C4ISR yang memiliki standar komunikasi dan keamanan ketat. Sistem sipil umumnya menggunakan protokol

komunikasi berbasis TCP/IP dan API terbuka, sementara sistem militer memanfaatkan jaringan tertutup dengan enkripsi tingkat tinggi seperti MIL-STD-1553 atau NATO STANAG 4586 untuk menjaga kerahasiaan dan keandalan data (Yang et al., 2021).

Salah satu solusi yang dapat diterapkan adalah penggunaan gateway interoperabilitas berbasis AI, yang dapat mengonversi format data sipil ke standar militer secara otomatis. Teknologi ini telah sukses diimplementasikan di Korea Selatan, di mana sistem *smart city* mereka terhubung dengan pusat komando militer untuk pengawasan *real-time* dan respons cepat terhadap ancaman (Albouq et al., 2022; Madjid et al., 2021).Di samping itu, keamanan siber menjadi elemen krusial dalam integrasi ini, mengingat Jakarta Smart City menghasilkan data strategis yang mencakup pergerakan transportasi, lokasi infrastruktur kritis, serta pola logistik kota.

Organisasi: Membangun Kolaborasi Yang Lebih Erat Antara Pengelola Jakarta Smart City Dan Instansi Pertahanan

Kolaborasi antara pengelola Jakarta Smart City dan instansi pertahanan sangat penting untuk memastikan bahwa sistem ini dapat digunakan secara efektif dalam konteks pertahanan. Kedua pihak perlu mengembangkan mekanisme kerja sama yang memungkinkan pertukaran informasi, sumber daya, dan tanggung jawab secara efisien. Menurut Ma et al. (2025), membentuk tim gabungan yang terdiri dari perwakilan kedua institusi dapat menciptakan jalur komunikasi yang lebih jelas dan mengurangi hambatan koordinasi. Pelatihan lintas sektor sangat diperlukan agar personel dari pemerintah daerah dan militer memiliki pemahaman yang sama mengenai teknologi C4ISR, manajemen keamanan data, serta pemanfaatan data *smart city* dalam operasi pertahanan.

Program pelatihan bisa mencakup simulasi penggunaan data *real-time* Jakarta Smart City dalam skenario militer atau penanggulangan krisis, yang telah terbukti efektif di negara-negara seperti Singapura dan Korea Selatan (Kendzierskyj & Jahankhani, 2020). Sebagai langkah lebih lanjut, pembangunan pusat komando gabungan dapat meningkatkan efektivitas koordinasi antara pemerintah sipil dan militer. Di Singapura, pusat komando gabungan berhasil mengintegrasikan sistem *smart city* dengan teknologi pertahanan, memungkinkan respons yang lebih cepat terhadap ancaman keamanan nasional (Tikanmäki et al., 2021). Jakarta dapat mengadopsi model ini dengan menyesuaikan kebutuhan lokal dan struktur organisasi yang ada.

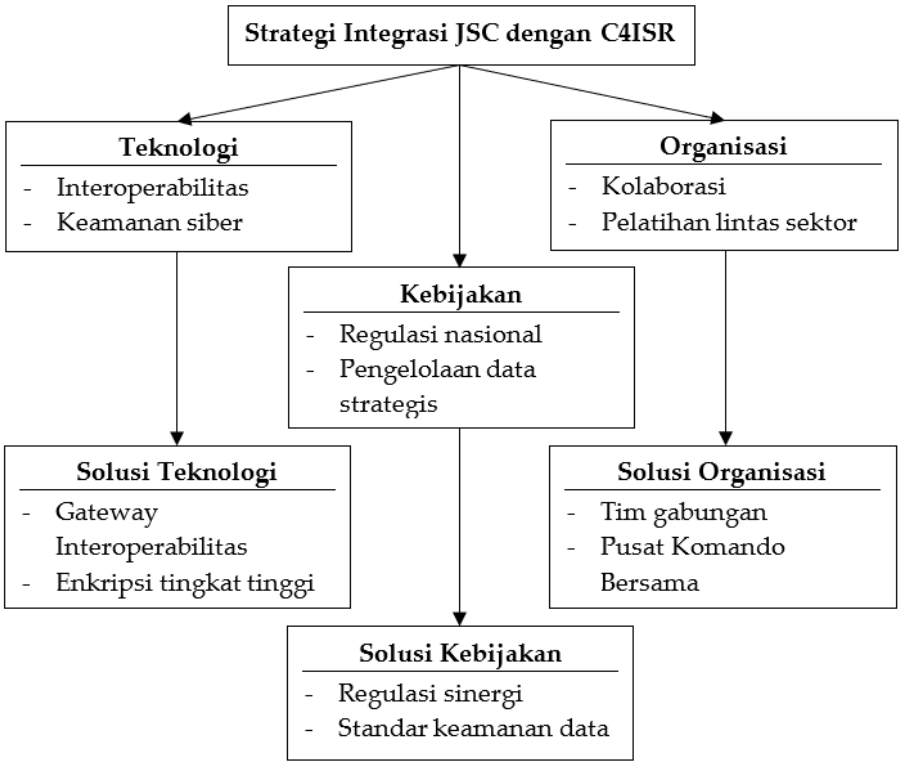
Kebijakan: Penyusunan Regulasi Nasional Yang Mendukung Sinergi Teknologi Sipil Dan Militer

Regulasi nasional memegang peran krusial dalam mendukung integrasi teknologi sipil dan militer, tetapi saat ini, Peraturan Gubernur No. 306 Tahun 2016 yang menjadi dasar hukum Jakarta Smart City belum mencakup aspek pertahanan negara. Menurut Lata & Kumar (2021), regulasi yang mendukung integrasi teknologi harus mencakup standar teknis, protokol keamanan, serta mekanisme koordinasi antarinstansi.

Regulasi baru juga perlu mengatur pengelolaan data strategis, memastikan bahwa informasi dari Jakarta Smart City hanya dapat diakses oleh instansi yang berwenang dan digunakan untuk kepentingan nasional. Studi dari Bommakanti (2020) menunjukkan bahwa kebijakan pengelolaan data yang jelas dapat mencegah penyalahgunaan informasi serta meningkatkan transparansi antarinstansi. Indonesia membutuhkan kerangka kerja kolaborasi lintas sektor di tingkat nasional yang mengatur peran pemerintah daerah, militer, serta sektor swasta dalam mendukung integrasi teknologi. Pengalaman dari Korea Selatan menunjukkan bahwa regulasi yang jelas dapat menciptakan sinergi yang efektif antara sektor sipil dan militer, sekaligus memperkuat keamanan nasional (Kim & Choi, 2016).

Beberapa langkah konkret yang dapat dilakukan meliputi menyesuaikan regulasi *smart city* agar mencakup kebijakan keamanan nasional dan pertahanan siber, mengembangkan standar interoperabilitas nasional yang mengacu pada NATO STANAG 4586 dan ISO 22301 (*Business Continuity Management*) untuk memastikan kelangsungan operasional dalam situasi darurat, dan membentuk badan pengawas independen yang bertanggung jawab terhadap integrasi *smart city* dan sistem pertahanan nasional. *Flowchart* pada Gambar 3 menggambarkan langkah-langkah utama dalam strategi integrasi ini, mulai dari peningkatan interoperabilitas dan keamanan siber, penguatan kolaborasi antarinstansi, hingga penyusunan regulasi nasional yang mendukung pengelolaan data strategis.

Gambar 3. Strategi Integrasi Jakarta Smart City dengan C4ISR



Sumber: Disusun oleh penulis

Strategi integrasi Jakarta Smart City dengan C4ISR memerlukan sinergi antara teknologi, organisasi, dan kebijakan. Di sisi teknologi, interoperabilitas sistem dan keamanan siber harus menjadi prioritas utama, dengan solusi seperti *gateway* interoperabilitas dan enkripsi tingkat tinggi. Dalam aspek organisasi, pembentukan tim gabungan dan pusat komando bersama dapat meningkatkan koordinasi lintas instansi, sementara pelatihan lintas sektor memperkuat pemahaman bersama. Di tingkat kebijakan, regulasi nasional yang komprehensif diperlukan untuk mengatur pengelolaan data strategis dan mendukung kolaborasi antara sektor sipil dan militer.

Keterbatasan dan Penelitian Masa Depan

Penelitian ini mengungkap potensi besar integrasi Jakarta Smart City dengan sistem C4ISR, tetapi masih ada beberapa keterbatasan yang perlu diperhatikan. Salah satu tantangan utama adalah minimnya akses terhadap data teknis dan sistem keamanan kedua *platform*, mengingat informasi pertahanan bersifat rahasia. Selain itu, perbedaan standar teknologi antara sistem sipil dan militer menjadi kendala dalam memastikan interoperabilitas yang aman dan efisien. Dari sisi kebijakan, belum adanya regulasi yang secara eksplisit mengatur sinergi *smart city* dengan sistem pertahanan membuat implementasi integrasi ini belum memiliki dasar hukum yang kuat.

Penelitian lebih lanjut perlu mengembangkan model simulasi integrasi berbasis *digital twin*, sehingga pengujian dapat dilakukan tanpa mengganggu sistem pertahanan yang sebenarnya. Selain itu, analisis keamanan siber yang lebih mendalam, termasuk pengujian penetrasi dan adopsi teknologi *blockchain* untuk perlindungan data, menjadi krusial. Dari aspek kebijakan, studi perbandingan dengan negara seperti Korea Selatan dan Singapura dapat memberikan wawasan tentang kerangka hukum yang memungkinkan sinergi teknologi sipil dan militer. Penelitian juga perlu mengeksplorasi kesiapan sumber daya manusia, termasuk pelatihan bagi operator *smart city* dan personel militer dalam memanfaatkan data berbasis AI dan IoT untuk mendukung strategi pertahanan. Dengan pendekatan ini, Jakarta Smart City tidak hanya menjadi solusi untuk tata kelola kota yang cerdas, tetapi juga komponen strategis dalam memperkuat pertahanan nasional di era digital.

6. Kesimpulan

Jakarta Smart City dapat menjadi contoh sukses integrasi teknologi sipil dan pertahanan, jika strategi ini diterapkan dengan baik memungkinkan pengambilan keputusan yang lebih cepat dan akurat dalam menghadapi ancaman keamanan. Bukan hanya sekadar *smart city*, tetapi juga kota yang siap menghadapi tantangan di era digital dengan sistem pertahanan yang lebih kuat dan berbasis data *real-time*.

Jakarta Smart City memiliki potensi besar untuk mendukung sistem C4ISR, terutama melalui pemanfaatan data transportasi, logistik, dan situasi darurat. Dengan infrastruktur teknologi yang terus berkembang, sistem ini mampu menyediakan data yang relevan untuk kebutuhan pertahanan negara. Namun, untuk memastikan integrasi ini berjalan lancar, diperlukan perhatian khusus pada interoperabilitas, keamanan data, dan pengembangan teknologi yang mendukung kolaborasi antara sektor sipil dan militer. Melalui strategi yang tepat, Jakarta Smart City dapat menjadi elemen penting dalam memperkuat sistem pertahanan negara.

Integrasi antara teknologi Jakarta Smart City dan sistem C4ISR menghadirkan tantangan. Kesenjangan teknologi, risiko keamanan data, dan koordinasi antarinstansi adalah hambatan utama yang harus diatasi untuk memastikan keberhasilan integrasi ini. Solusi yang dapat diterapkan meliputi pengembangan protokol teknis bersama untuk meningkatkan interoperabilitas, penguatan sistem keamanan siber untuk melindungi data sensitif, dan pembaruan regulasi untuk memfasilitasi kolaborasi antara pemerintah daerah dan militer. Dengan pendekatan yang holistik dan terarah, tantangan-tantangan ini dapat diatasi, sehingga integrasi ini mampu memberikan manfaat optimal bagi pertahanan dan keamanan nasional.

Integrasi antara teknologi Jakarta Smart City dan sistem C4ISR memerlukan strategi yang holistik. Di bidang teknologi, peningkatan interoperabilitas sistem dan penguatan keamanan siber adalah langkah utama. Dalam aspek organisasi, membangun kolaborasi yang erat melalui tim gabungan, pelatihan lintas sektor, dan pusat komando bersama dapat memperkuat hubungan antara pengelola *smart city* dan instansi militer. Sementara itu, di ranah kebijakan, regulasi nasional yang mendukung sinergi teknologi sipil dan militer menjadi elemen yang tidak dapat diabaikan. Dengan pendekatan yang tepat, Jakarta Smart City dapat menjadi elemen strategis dalam mendukung keamanan nasional.

Referensi

Albouq, S., Abi Sen, A., Almashf, N., Yamin, M., Alshanqiti, A., & Bahbouh, N. (2022). A Survey of Interoperability Challenges and Solutions for Dealing With Them in IoT Environment. *IEEE Access*, *10*, 1. https://doi.org/10.1109/ACCESS.2022.3162219

Batty, M. (2018). Artificial intelligence and smart cities. *Environment and Planning B: Urban Analytics and City Science*, *45*(1), 3–6. https://doi.org/10.1177/2399808317751169

Belli, L., Cilfone, A., Davoli, L., Ferrari, G., Adorni, P., Di Nocera, F., Dall'Olio, A., Pellegrini, C., Mordacci, M., & Bertolotti, E. (2020). IoT-enabled smart sustainable cities: Challenges and approaches. *Smart Cities*, *3*(3), 1039–1071. https://doi.org/10.3390/smartcities3030052

Bitzinger, R. A. (2021). China's shift from civil-military integration to military-civil fusion. *Asia Policy*, *16*(1), 5–24. https://www.rsis.edu.sg/wp-content/uploads/2022/05/Asia-Policy-16.1-Jan-2021-Richard-Bitzinger.pdf

Bommakanti, K. (2020). *Strengthening the C4ISR Capabilities of India's Armed Forces: The Role of Small Satellites*. https://www.researchgate.net/publication/342170938

Caňares, M. P. (2018). *The Social Dynamics of Open Data edited by François van Schalkwyk, Stefaan G Verhulst, Gustavo Magalhaes, Juan Pane & Johanna Walker*. Project Muse. https://library.oapen.org/bitstream/handle/20.500.12657/28912/9781928331568_txt.pdf?sequence=1#page=175

Chen, L., Chen, P., & Lin, Z. (2020). Artificial intelligence in education: A review. *Ieee Access*, *8*, 75264–75278.

Choi, C., Choi, J., Kim, C., & Lee, D. (2020). The smart city evolution in South Korea: Findings from big data analytics. *Journal of Asian Finance, Economics and Business*, *7*(1), 301–311. https://doi.org/10.13106/jafeb.2020.vol7.no1.301

Creswell, J. W. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (4th ed.)*. SAGE Publications. https://us.sagepub.com/en-us/nam/qualitative-inquiry-and-research-design/book266033

Department of Defense. (2024). *Cybersecurity Maturity Model Certification (CMMC) Model Overview Cybersecurity Maturity Model Certification (CMMC) Model Overview / Version 2.13 ii NOTICES*. https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview.pdf

Diskominfo. (2016). *GUBERNUR PROVINSI DAERAH KHUSUS IBUKOTA JAKARTA*. https://www.diskom.info/jakarta/uploads/download/PERGUB_NO_306_TAHUN_2016_-_OTK_UP_JSC.pdf

European Union Agency for Cybersecurity (ENISA). (2021). *About ENISA – The EU Cybersecurity Agency. European Union.* https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/european-union-agency-cybersecurity-enisa_en

Hanggara, A. G. (2021, April 26). *Mengintip Teknologi yang Digunakan Jakarta Smart City*. Jakarta Smart City. https://smartcity.jakarta.go.id/id/blog/mengintip-teknologi-yang-digunakan-jakarta-smart-city/

Houichi, M., Jaidi, F., & Bouhoula, A. (2024). Cyber Security within Smart Cities: A Comprehensive Study and a Novel Intrusion Detection-Based Approach. *Computers, Materials and Continua*, *81*(1), 393–441. https://doi.org/https://doi.org/10.32604/cmc.2024.054007

Hutomo, A., Putro, I. N. Y., Qomariyah, L., Ningsih, S. J., Wadjdi, A. F., Lestari, A. A., Gultom, R. A. G., Purwantoro, S. A., Widodo, P., & Amperiawan, G. (2021). Evaluating the Interoperability of C4ISR System using Cyber Six-ware Framework. *2021 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, 1–7. https://doi.org/10.1109/ICACSIS53237.2021.9631359

Wisnubroto, K. (2024, August 16). *Makan bergizi gratis dan renovasi sekolah unggulan pemerintah di 2025*. Indonesia.go.id. https://indonesia.go.id/kategori/editorial/8507/makan-bergizi-gratis-dan-renovasi-sekolah-unggulan-pemerintah-di-2025?lang=1.

International Organization for Standardization. (2020). *ISO/IEC 27001: Information security management systems – Requirements.* ISO. https://www.iso.org/standard/54534.html

Izzuddin, F. (2022). KONSEP SMART CITY DALAM PEMBANGUNAN BERKELANJUTAN. *Citizen : Jurnal Ilmiah Multidisiplin Indonesia*, *2*, 376–382. https://doi.org/10.53866/jimi.v2i3.96

Jakarta Smart City. (2023). *Daftar Isi Menuju Kota Cerdas Berskala Global 7*. www.smartcity.jakarta.go.id

Kim, S. J., & Choi, D. Y. (2016). The development of regulatory management systems in East Asia: Country studies. *Economic Research Institute for ASEAN and East Asia (ERIA)*. https://www.eria.org/RPR_FY2015_No.4_Chapter_4.pdf

Keenan, J. M., Trump, B., Kytömaa, E., Adlakha-Hutcheon, G., & Linkov, I. (2024). The role of science in resilience planning for military-civilian domains in the US and NATO. *Defence Studies*, 1–32. https://doi.org/10.1080/14702436.2024.2365218

Kendzierskyj, S., & Jahankhani, H. (2020). Critical National Infrastructure, C4ISR and Cyber Weapons in the Digital Age. In H. Jahankhani, S. Kendzierskyj, N. Chelvachandran, & J. Ibarra (Eds.), *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity* (pp. 3–21). Springer International Publishing. https://doi.org/10.1007/978-3-030-35746-7_1

Kim, K., Alshenaifi, I. M., Ramachandran, S., Kim, J., Zia, T., & Almorjan, A. (2023). Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey. In *Sensors* (Vol. 23, Issue 7). MDPI. https://doi.org/10.3390/s23073681

König, P. D. (2021). Citizen-centered data governance in the smart city: From ethics to accountability. *Sustainable Cities and Society*, *75*, 103308. https://doi.org/https://doi.org/10.1016/j.scs.2021.103308

Kulve, H. te, & Smit, W. A. (2003). Civilian–military co-operation strategies in developing new technologies. *Research Policy*, *32*(6), 955–970. https://doi.org/https://doi.org/10.1016/S0048-7333(02)00105-1

Lata, M., & Kumar, V. (2021). Standards and regulatory compliances for IoT security. *International Journal of Service Science, Management, Engineering, and Technology*, 12(3), 133–147. https://doi.org/10.4018/IJSSMET.2021090109

Lebang, C. G., Priyandita, G., Wijaya, T., Zakaria, N. A., Alham, D., & Rasyid, K. (2023). *TRANSFORMASI DIGITAL INDONESIA Kondisi Terkini dan Proyeksi Penulis Asisten Penulis*. https://img.lab45.id/images/article/2023/11/28/257/829transformasi-digital-indonesia-kondisi-terkini-dan-proyeksish.pdf

Ma, C., Song, M., Zeng, W., Wang, X., Chen, T., & Wu, S. (2025). Enhancing urban emergency response: A Euclidean distance-based framework for optimizing rescue facility layouts. *Sustainable Cities and Society*, *118*, 106006. https://doi.org/https://doi.org/10.1016/j.scs.2024.106006

Made, N., & Mahayani, H. (2024). Evaluasi implementasi smart city di Indonesia: Tantangan teknologi dan keberlanjutan. *GOVERNANCE: Jurnal Ilmiah Kajian*

Politik Lokal dan Pembangunan. https://governance.lkispol.or.id/index.php/description/article/view/209/201

Madjid, M. A., Legionosuko, T., & Samudro, E. G. (2021). The information security strategy of Bogor's smart city to deal with threat in cyber space. *IOP Conference Series: Materials Science and Engineering*, *1073*(1), 012054. https://doi.org/10.1088/1757-899x/1073/1/012054

Ng, J. (2022, June 14). *Taking on C4ISR and Cyber*. Asian Military Review. https://www.asianmilitaryreview.com/2022/06/taking-on-c4isr-and-cyber/

NIST. (2021). *National Initiative for Cybersecurity Education (NICE)*. National Institute of Standards and Technology. https://www.nist.gov/itl/applied-cybersecurity/nice

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*(1), 1609406917733847. https://doi.org/10.1177/1609406917733847

Panda. (2023, December 26). *Meningkatkan Koordinasi dan Kerjasama Antar Lembaga Pemerintah Daerah dalam Teknologi Tepat Guna: Membangun Ekosistem yang Kondusif*. Panda. https://www.panda.id/meningkatkan-koordinasi-dan-kerjasama-antar-lembaga-pemerintah-daerah-dalam-teknologi-tepat-guna-membangun-ekosistem-yang-kondusif/

Perera, C., Liu, C. H., & Jayawardena, S. (2015). The emerging internet of things marketplace from an industrial perspective: A survey. *IEEE Transactions on Emerging Topics in Computing*, *3*(4), 585–598. https://doi.org/10.1109/TETC.2015.2390034

Rifaid, R., Abdurrahman, A., Baharuddin, T., & A. Kusuma, B. M. (2023). Smart City Development in the New Capital City: Indonesian Government Plans. *Journal of Contemporary Governance and Public Policy*, *4*(2), 115–130. https://doi.org/10.46507/jcgpp.v4i2.141

Sarjito, I. A. (2023). *Kebijakan dan Strategi Pertahanan*. CV Jejak (Jejak Publisher). https://catalogue.nla.gov.au/catalog/10016621?utm_source=chatgpt.com

Sumari, A. (2014). *Cyberspace Operations and C4ISR*. https://doi.org/10.13140/RG.2.2.35827.17445

Susantono, B., Berawi, M. A., & Sari, M. (2024). Smart City Framework for Nusantara Capital City Development. In *The Emerald Handbook of Smart Cities in the Gulf Region: Innovation, Development, Transformation, and Prosperity for Vision 2040*

(pp. 481–514). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83608-292-720241032

Tikanmäki, I., Räsänen, J., Ruoslahti, H., & Rajamäki, J. (2021). Maritime Surveillance and Information Sharing Systems for Better Situational Awareness on the European Maritime Domain: A Literature Review. In T. Tagarev, K. T. Atanassov, V. Kharchenko, & J. Kacprzyk (Eds.), *Digital Transformation, Cyber Security and Resilience of Modern Societies* (pp. 117–135). Springer International Publishing. https://doi.org/10.1007/978-3-030-65722-2_8

West, D. M. (2018). *The future of work: Robots, AI, and automation*. Brookings Institution Press. https://www.researchgate.net/publication/329877216_The_future_of_work_Robots_AI_and_automation

Yang, J., Kwon, Y., & Kim, D. (2021). Regional Smart City Development Focus: The South Korean National Strategic Smart City Program. *IEEE Access*, *9*, 7193–7210. https://doi.org/10.1109/ACCESS.2020.3047139

Zhang, J., Pan, L., Han, Q.-L., Chen, C., Wen, S., & Xiang, Y. (2021). Deep learning based attack detection for cyber-physical system cybersecurity: A survey. *IEEE/CAA Journal of Automatica Sinica*, *9*(3), 377–391.