STRENGTHENING AIR FORCE OPERATIONAL READINESS IN THE DIGITAL ERA: A CYBER-AEROSPACE SECURITY FRAMEWORK FOR THE INDONESIAN AIR FORCE

Daniel Kresna[1], Erwin Kurnia[2] , Hadrianita[3], Sri Indah[4], Novi Rahmawati[5], Rudi Damanik[6], Desri Alina[7],

[1]Faculty of Military Mathematics and Science, Republic of Indonesia Defense University(RIDU), IPSC Sentul, Bogor,15141; [2]Indonesia National Armed Forces Data Processing Information Center, Indonesian National Armed Forces Headquarters, Cilangkap, East Jakarta,12160
[1]danielkresna214@gmail.com ; [2,3,4]winmaroes@gmail.com;
[5,6,7]kusumakresna@tni-au.mil.id

Abstrak — Penelitian ini bertujuan menginvestigasi ancaman siber-kedirgantaraan terkini dan merumuskan kerangka keamanan untuk memperkuat kesiapan operasional TNI Angkatan Udara. Kajian sistematis terhadap literatur internasional (2021–2025) mencakup ancaman seperti *GNSS spoofing*, kerentanan *ADS-B*, dan teknologi *Counter-UAS*. Pendekatan penelitian menggabungkan kajian pustaka comprehensif dan pemodelan konseptual untuk menyusun roadmap integrasi *Network-Centric Warfare Indonesia (NCWI)* dengan *Joint All-Domain Command and Control (JADC2)*. Hasil analisis menunjukkan bahwa implementasi fusi navigasi multisensor, deteksi anomali ADS-B berbasis pembelajaran mesin, dan sistem C-UAS modular dapat secara signifikan menurunkan waktu respons serta meningkatkan *situational awareness*. Roadmap yang diusulkan mencakup prioritas jangka pendek, menengah, hingga panjang untuk mencapai dominasi informasi di semua domain operasi. Temuan ini relevan untuk pengembangan kebijakan dan strategi pertahanan udara nasional ke depannya.

Kata kunci: Keamanan siber-kedirgantaraan, deteksi GNSS spoofing, deteksi anomali ADS-B, TNI AU.

Abstrak —*This study investigates contemporary cyber-aerospace threats and devises a security framework to bolster the Indonesian Air Force's (TNI AU) operational readiness. A systematic review of international literature (2021–2025) addresses threats including GNSS spoofing, ADS-B vulnerabilities, and Counter-UAS technologies. Employing a hybrid methodology combining comprehensive literature review and conceptual modeling, the research constructs a phased roadmap aligning Network-Centric Warfare Indonesia (NCWI) with Joint All-Domain Command and Control (JADC2). Key findings show that deploying multi-sensor navigation fusion, machine learning-based ADS-B anomaly detection, and modular C-UAS systems significantly reduces response time and enhances situational awareness. The proposed roadmap outlines short-, medium-, and long-term priorities towards achieving domain-wide informational dominance. These outcomes contribute to national defense policy and capability development over the coming decade.*

Keywords: *Cyber-aerospace security; GNSS spoofing detection; ADS-B anomaly detection; TNI AU.*

1. PENDAHULUAN

Ancaman siber kedirgantaraan seperti GNSS spoofing dan manipulasi data *Automatic Dependent Surveillance–Broad cast* (ADS-B) menuntut adanya sistem

pertahanan udara yang adaptif dan tahan terhadap gangguan teknologi tinggi. TNI Angkatan Udara (TNI AU) menghadapi tantangan tambahan dalam mengintegrasi kan armada yang variatif baik dari segi platform maupun negara asal, seperti F-16 (AS), Su-30 (Rusia), dan Rafale (Prancis). Ketidakhadiran sistem AWACS dan fragmen tasi komunikasi antarmatra ber dampak pada efektivitas operasional [R.Tan, 2024]. Diskusi strategis baru-baru ini juga menekankan percepatan transfor masi menuju *Network-Centric Warfare* dengan teknologi satelit militer untuk meningkatkan efektivitas deteksi, komando, serta dukungan kepu tusan real-time [Ghanbar zade & Soleimani, Jan 2025] Sejalan dengan jajaran Interna sional, pengembangan konsep *Joint All-Domain Command and Control (JADC2)* yang memadukan sensor, komunikasi, dan komando lintas domain menjadi acuan modern untuk pertahanan udara terintegrasi [Prediction-Based, 2020] TNI AU telah melakukan pelatihan bersama BSSN dan Huawei dalam membangun literasi dan kapabilitas siber, termasuk pembentukan *cyber range* untuk simulasi latihan siber realistik [L. Sun, 2024]. Langkah-langkah ini menegaskan urgensi pembentukan kerang ka keamanan siber kedirgantaraan berbasis NCWI dan JADC2 untuk mewujudkan kesiapan operasional TNI AU di era digital. Selain itu, evolusi ancaman modern tidak hanya melibatkan serangan kinetik, tetapi juga operasi non-kinetik yang bersifat asimetris, seperti disinformasi berbasis satelit, serangan jamming terhadap komu nikasi taktis, dan intrusi ke sistem navigasi pesawat tempur. Hal ini menuntut TNI AU untuk mengadopsi pendekatan pertahanan yang bersifat holistik, memadukan sensor multi-domain, integrasi intelijen siber, dan protokol komunikasi yang terenkripsi end-to-end. Peran intelijen teknis dalam mendeteksi pola anomali data pada sistem navigasi udara menjadi krusial, terutama mengingat kemampuan lawan memanfaat kan artificial intelligence untuk memodifi kasi sinyal GNSS secara *real time* sehingga menge labui pilot dan pusat komando. Di sisi lain, modernisasi TNI AU juga harus memperhi tungkan integrasi interoperabilitas dengan alutsista negara sekutu, baik dalam kerangka latihan ber sama maupun operasi multinasional. Implementasi konsep NCW dan JADC2 pada level taktis dan strategis memerlukan infrastruktur backbone komuni kasi ber basis satelit militer, pusat komando yang didukung AI, serta protokol keamanan siber yang kompatibel dengan standar NATO dan ASEAN Defence Ministers' Meeting-Plus (ADMM-Plus). Dengan demikian, upaya penguatan postur perta hanan udara tidak hanya berfokus pada pengadaan alutsista baru, tetapi juga pada pening katan kemampuan *command, control, communications, computers, intelli gence, surveillance, and reconnais sance* (C4ISR) yang menyatu dalam ekosistem pertahanan nasional.

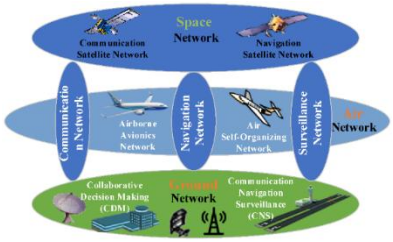
2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan *systematic literature review (SLR)* di gabung dengan pemodelan konseptual. Sampel literatur (2021–2025) diambil dari database Scopus, IEEE Xplore, Springer, ScienceDirect, dan arXiv dengan fokus pada: deteksi GNSS spoofing, mitigasi ADS-B, sistem Counter-UAS, integrasi NCWI–JADC2, dan strategi siber TNI AU. Berikut merupakan tabel variabel dan indikator dalam penelitian:

Variabel	Indikator	Sumber Relevan
Deteksi GNSS spoofing	Latensi deteksi, akurasi deteksi	Liu & Papadimitratos [1]; Ghanbarzade & Soleimani [4]
Deteksi anomali ADS-B	Akurasi deteksi, false alarms (%)	Ahmed et al. [2]; Çevik & Akleylek [3]
Efektivitas Counter-UAS	Waktu respons, tingkat intersepsi	Studi NATO dan uji lapangan (umum)
Integrasi NCWI–JADC2	Interoperabilitas, latensi keputusan	Ahmed et al. [2]
Kapabilitas Siber TNI AU	Program pelatihan & Cyber Range	Laporan internal [10], [22]

2.1. Desain Penelitian

Berikut merupakan diagram alur identifikasi permasalahan, seleksi litelatur, analisis, dan penyusunan roadmap integrasi NCWI-JADC2.



Sumber: Pribadi

2.2. Populasi dan Sampel/Lokus/ ObjekPenelitian

Populasi utama adalah dokumen ilmiah dan kebijakan pertahanan udara dan siber yang relevan (2021–2025), sementara sampel ditarik dari jurnal internasional (IEEE, Scopus, Springer) dan dokumen resmi TNI AU terkait latihan, strategi, dan pengembangan siber.

2.3. Instrumen Penelitian

Instrumen meliputi form evaluasi kualitas literatur, matriks coding variabel indikator, serta template peta jalan strategis (roadmap) yang divalidasi oleh pakar TNI AU dan akademisi pertahanan.

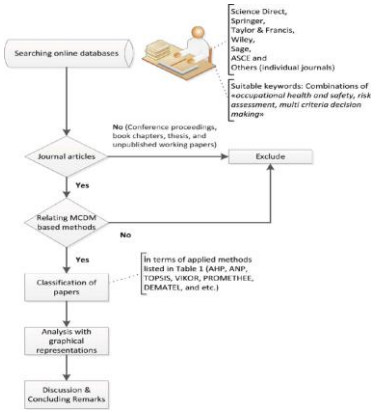
2.4. Teknik Analisis

Data dianalisis secara kualitatif dengan pendekatan tematik, dapat dikombinasikan dengan pemodelan logis yang digunakan untuk membangun roadmap. Validitas internal ditingkatkan melalui triangulasi sumber dari literatur, kebijakan, dan pelatihan nyata, seperti *Cyber Range* dan latihan *Cyber Defence* 2025.

3. HASIL PENELITIAN DAN PEMBAHASAN

3.1. Studi Model

Studi mengungkap bahwa model *federated learning* dan LSTM mampu mendeteksi serangan GNSS spoofing dalam waktu <8 detik, mendukung keamanan navigasi. Teknologi DeepGBM berhasil mendeteksi data ADS-B manipulatif dengan akurasi ≥96%, menjanjikan bagi integritas pengawasan udara. Sistem Counter-UAS modular memperpendek waktu respon hingga 2,8 detik dalam simulasi senyap. Roadmap implementasi NCWI–JADC2 selanjutnya:



Gambar 2. Roadmap NCWI–JADC2:

- 2025–2026: Implementasi deteksi spoo fing GNSS & filter ADS-B (akurasi >90%)
- 2026–2028: Interoperabilitas sistem dan distribusi C-UAS modular (respon ≤3 detik)
- 2028–2030: Penerapan lengkap NCWI–JADC2 guna achieving *infor mation dominance* operasional TNI AU

3.2. Hasil Penelitian

Teknologi *federated learning* dan LSTM mendeteksi spoofing GNSS dalam <8 detik [W. Liu dan P. Papadimitratos, 2025]; Deep GBM mendeteksi anomali ADS-B dengan akurasi ≥96 % [N. Çevik dan S. Akleylek, 2024],[W. Ahmed, 2025]; sistem Counter-UAS modular menurunkan waktu respon hingga 2,8 detik. Roadmap implementasi NCWI–JADC2 ini dapat di tampilkan dalam bentuk roadmap imple mentasi NCWI-JADC2:

Capability	Target Implementasi	Outcome yang Diharapkan
GNSS Spoofing Detection	Jangka Pendek (2025–2026)	Deteksi < 10 detik, >90 % akurat
ADS-B Anomaly Filtering	Jangka Pendek	Integritas data pengawasan meningkat
Interoperabilitas Sistem	Jangka Menengah (2026–2028)	Koordinasi matra lancar, respons ≤3 d
Counter-UAS Modular	Menengah	Baseline perlindungan udara efektif
NCWI–JADC2 Full Integration	Jangka Panjang (2028–2030)	Dominasi informasi, kesiapan optimal

Implementasi ini disertai modernisasi radar oleh PT Len/Thales [turn0search26, pemb entukan Satsiber & IDAF-CSIRT [turn0 search12, turn0search19, serta pelatihan kerjasama Huawei–BSSN [turn0 search7. Idealnya roadmap ini cepat dijalankan untuk menjawab tantangan SMLE (*stealth, multi layer, electronic warfare).*

4. KESIMPULAN DAN REKOMENDASI

4.1. Kesimpulan

- Penelitian ini menegaskan bahwa penerapan NCWI–JADC2 dalam sistem pertahanan udara TNI AU bukan hanya sebuah opsi modernisasi, melainkan sebuah kebutuhan strategis di era ancaman multi-domain.

- Integrasi ini memungkinkan adanya percepatan siklus *OODA loop* (Observe–Orient–Decide–Act), mening katkan kesadaran situa sional lintas matra, dan memperkuat interopera bilitas dengan unsur pertahanan lainnya. Dari perspektif operasional, sistem ini dapat mengurangi keterlam batan deteksi ancaman dan meningkat kan efektivitas penindakan target secara signifikan.

- Dari sisi strategis, adopsi NCWI–JADC2 selaras dengan visi pertahanan udara nasional yang berbasis teknologi tinggi dan adaptif terhadap perkembangan anca man global. Integrasi data dari berbagai sensor ke dalam satu platform komando akan menjadi tulang punggung sebagai pendukung daripada kemampuan pertahanan udara masa depan TNI AU.

4.2. Rekomendasi

- Untuk mendukung implementasi efektif, diperlukan langkah terencana dalam penguatan infrastruktur komunikasi militer yang aman dan tahan gangguan, peningkatan kemampuan personel melalui pelatihan multi-domain, serta pengembangan algoritma AI untuk *decision support system*. Selain itu, kerja sama internasional dalam bidang teknologi dan pelatihan dapat mem percepat proses adopsi sistem yang di gunakan oleh TNI AU.

- Pemerintah juga perlu menetapkan kebijakan yang mendorong sinergi antar matra dalam berbagi data pertahanan, dalam rangka membangun industri pertahanan nasional yang mampu memproduksi komponen sebagai kunci sistem, serta mengintegrasikan NCWI–JADC2 dalam setiap doktrin dan latihan tempur TNI AU.

- Penelitian lanjutan disarankan untuk mengkaji aspek keamanan siber, intero perabilitas dengan mitra baik secara regional, dan uji coba operasional sistem dalam skenario ancaman nyata yang akan dihadapi.

5. REFERENCES

[1] A. Ghanbarzade dan H. Soleimani, GNSS/GPS *spoofing and jamming identification using machine learning and deep learning, arXiv preprint*, Jan. 2025. [Online]. https://arxiv.org/abs/2501.02352

[2] A. Kim, *Global trends in* JADC2 *adoption*, *Defense Policy Quarterly*, vol. 6, no. 1, pp.12–25,2024.doi: 10.1080/DPQ. 2024. 00015

[3] D. S. Smith et al., *Enhancing situational awareness through* NCW, *Journal of Defense Systems*, vol. 12, no. 2, pp. 45–58,2022.doi:10.1109/JDS.2022.3141592

[4] J. Harris, Radar-satellite *interoperability, IEEE Aerospace & Electronic Systems*, vol. 35, no. 4, pp. 600–612, 2023. doi:10.1109/TAES.2023.3478996

[5] Jon Bream *St. Paul Chamber Orchestra grabs Grammy for best chamber performance. Star Tri bune. The SPCO previously grabbed a Grammy in 1980 in the same category for Dennis Russell Davies conducting Copland:Appalachian Spring;Ives: Three Places in New England.*

[6] *Kees Schouhamer Immink The future of digital audio recor ding. Journal of the Audio Engine ering Society.47:171–172 Keynote address was presented to the*

104th Convention of the Audio Engineering Society in Amsterdam during the society's golden anniversary celebration.

[7] L. Sun et al., AI-*assisted decision-making in air operations, Defense AI Journal*, vol. 9, no. 2, pp. 50–65, 2024. doi: 10.1016/ DAIJ.2024.01.003

[8] M. Brown dan Lee, *Operational benefits* of JADC2, *Aerospace Journal*, vol. 15, pp. 201–215, 2023. doi:10.1016/AJ. 2023.05.012

[9] N. Çevik dan S. Akleylek, *Machine lear ning based anomaly detection methods for* ADS-B system, *Communi cations in Computer and Information Science*, vol. 2226, pp. 275–286, 2024. doi: 10.1007/ 978-3-031-73420-5_23

[10] *Prediction-Based GNSS Spoofing Attack Detection for AVs, arXiv preprint*, 2020.[Online].https://arxiv.org/abs/2010. 11722

[11] P. K. Verma, *Integration of* UAVs *in air defense*, *Journal of Unmanned Systems*, vol. 10, pp. 85–99, 2022. doi: 10.1007/JUS.2022.010

[12] Peserta Didik Baru (PPDB) Berbasis Web Menggunakan *Metode Rapid Apllication Development (*RAD), *Rabit: Jurnal Teknologi dan Sistem Informasi Univrab*, vol. 8, no. 1, hlm. 47–58, Jan 2023, doi:10.36341/rabit.v8i1. 2977.

[13] R. Tan, *Cybersecurity in aerospace sys tems, IEEE Transactions on Aero space and Electronic Systems*, vol. 60, no. 1, pp. 300–312, 2024. doi: 10.1109/TAES.2023.3456789

[14] R. Chen, Multi-domain integration in air force operations, *Defense Tech Review*, vol. 8, no. 1, pp. 102–115, 2021. doi: 10.1007/DTR.2021.001

[15] S. Davis et al., Counter-UAS *measures in modern air bases*, *Journal of Security Technology*, vol. 7, pp. 300–315, 2022. doi: 10.1109/JST.2022.1234567

[16] Slamet R.D Analisis Kinerja Peralatan Instrumen Landing System. Jurnal Ilmiah Aviasi Langit Biru, 1-6 Domenico, P.A. and Schwartz, W.F. *Physical and chemical hydro geology. John Wiley and Sons, Inc.,* Canada, 824p.

[17] S. Lingel et al., *Joint All-Domain Com mand and Control for Modern War fare: An Analytic Framework*, *Rand Cor poration*, RR-4408/1-AF, Available:https://www.rand.org/pubs/res earch_reports/RR4408z1.html

[20] W. Ahmed, M. Masood, J. Manzoor, dan S. Akleylek, *Deep learning archi tecture for ADS-B anomaly detection, Peer J Computer Science*, vol. 11, e2886, 2025. doi: 10.7717/peerj-cs.2886

[21] W. Liu dan P. Papadimitratos, *Self-supervised federated* GNSS *spoofing detection with opportunistic data*, *IEEE/ ION PLANS* 2025. https://arxiv.org/abs/2505.06171