STRATEGI PERTAHANAN MILITER INDONESIA DALAM MENGHADAPI ANCAMAN ASYMMETRIC CYBER WARFARE DI ERA DIGITAL

Abid Taufiqur Rohman*
Informatika, Fakultas Sains dan Teknologi, Universitas Teknologi Yogyakarta
*abidtaufiqur@gmail.com

ABSTRAK

Ruang siber saat ini telah berevolusi menjadi dimensi pertempuran baru yang secara radikal mengubah doktrin keamanan global. Pergeseran paradigma ini ditandai dengan ancaman serangan destruktif terhadap infrastruktur vital yang tidak lagi mengandalkan kekuatan kinetik, melainkan barisan kode berbahaya (malware) yang dikendalikan dari jarak jauh tanpa kontak fisik. Merespons dinamika tersebut, penelitian ini mengevaluasi kesiapan doktrin pertahanan militer Indonesia saat ini menggunakan metode kualitatif melalui pendekatan deskriptif-analitis dan studi kepustakaan. Hasil kajian menunjukkan bahwa postur pertahanan yang berpusat pada matra konvensional dan memposisikan siber sekadar sebagai fungsi pendukung berpotensi menciptakan kerentanan taktis. Ketiadaan matra siber yang otonom membatasi ruang gerak komando penindakan yang agresif. Oleh karena itu, penelitian ini merekomendasikan adopsi doktrin *Active Cyber Defense* yang diintegrasikan dengan filosofi Sistem Pertahanan dan Keamanan Rakyat Semesta (Sishankamrata) melalui skema *Digital Pentahelix*. Kolaborasi ini menempatkan militer sebagai ujung tombak penindakan ancaman intensitas tinggi, sementara sektor sipil dan swasta berperan sebagai sistem peringatan dini dan ruang penyangga. Pembentukan matra siber yang mandiri dan harmonisasi yurisdiksi menjadi urgensi demi menjaga kedaulatan negara Republik Indonesia di ruang nirkontak.

Kata-kunci: *active defense; angkatan siber; asymmetric warfare; ruang siber; sishankamrata.*

INDONESIA'S MILITARY DEFENSE STRATEGY IN FACING THE THREAT OF ASYMMETRIC CYBER WARFARE IN THE DIGITAL ERA

ABSTRACT

Cyberspace has currently evolved into a new dimension of battle that radically alters global security doctrines. This paradigm shift is characterized by the threat of destructive attacks on vital infrastructure that no longer rely on kinetic force, but rather on malicious codes (malware) controlled remotely without physical contact. Responding to these dynamics, this study evaluates the readiness of Indonesia's current military defense doctrine using a qualitative method through a descriptive-analytical approach and literature review. The results indicate that a defense posture centered on conventional domains and positioning cyber merely as a supporting function potentially creates tactical vulnerabilities. The absence of an autonomous cyber domain limits the operational space for aggressive command responses. Therefore, this study recommends the adoption of an Active Cyber Defense doctrine integrated with the Total People's Defense and Security System (Sishankamrata) philosophy through a Digital Pentahelix scheme. This collaboration positions the military as the spearhead against high-intensity threats, while the civil and private sectors act as early warning systems and buffer zones. The establishment of an independent cyber force and harmonization of jurisdiction are absolute urgencies to maintain the sovereignty of the Republic of Indonesia in the contactless space.

Keywords*: active defense; asymmetric warfare; cyber force; cyberspace; sishankamrata.*

PENDAHULUAN

Seiring dengan pesatnya perkembangan teknologi informasi, paradigma ancaman keamanan nasional dan global telah mengalami pergeseran fundamental (Budi et al., 2021). Ruang siber kini telah diakui secara luas sebagai dimensi pertempuran baru yang tak kasat mata, melengkapi tiga matra pertahanan konvensional yakni darat, laut, dan udara. Dalam doktrin militer modern, ancaman terhadap kedaulatan tidak lagi didominasi oleh invasi kekuatan fisik atau pengerahan alutsista konvensional secara frontal (Heller, 2021). Sebaliknya, perang modern semakin diwarnai oleh taktik *asymmetric warfare*, di mana ruang siber menjadi instrumen utama untuk melumpuhkan infrastruktur kritis, memanipulasi informasi, hingga meruntuhkan stabilitas suatu negara tanpa harus melepaskan satu butir peluru pun (Khan, 2025).

Karakteristik utama dari *asymmetric cyber warfare* adalah ketidakseimbangan sumber daya, di mana aktor dengan kekuatan militer atau logistik yang jauh lebih kecil seperti aktor non-negara, hacktivist, atau proksi siber mampu memberikan dampak destruktif berskala masif terhadap angkatan bersenjata yang lebih superior. Hal ini terbukti dari berbagai insiden global. Salah satu preseden paling bersejarah adalah serangan *malware Stuxnet*, sebuah senjata siber yang sukses melumpuhkan sentrifugal fasilitas nuklir Iran secara fisik (Christello, 2025). Lebih lanjut, dalam konflik kontemporer seperti invasi Rusia ke Ukraina, militer Rusia menggunakan malware perusak seperti *Fox-Blade* untuk melumpuhkan jaringan komando dan kontrol (C2) serta sistem radar Ukraina sesaat sebelum serangan fisik dilancarkan (Sharma, 2025). Serangan semacam ini, yang sering disebut sebagai *shadow strikes*, memungkinkan penyerang beroperasi dalam anonimitas namun berdampak layaknya rudal balistik (Yu et al., 2025).

Bagi Indonesia, eskalasi ancaman *asymmetric cyber warfare* ini menuntut transformasi strategi pertahanan yang adaptif. Sebagai negara dengan tingkat digitalisasi yang tinggi namun masih menghadapi tantangan kerentanan infrastruktur strategis, Tentara Nasional Indonesia (TNI) dituntut untuk tidak hanya mengandalkan pendekatan pertahanan fisik (Prasetyo et al., 2026). Konsep Sistem Pertahanan dan Keamanan Rakyat Semesta perlu direvitalisasi dan diperluas ke dalam ruang dimensi siber (Tarom, 2025). Oleh karena itu, penguatan doktrin *active cyber defense*, pengembangan sumber daya manusia khusus di matra siber, serta sinergi sipil-militer menjadi sebuah urgensi mutlak demi menjaga kedaulatan negara Republik Indonesia di era digital.

Di tingkat domestik, eskalasi ancaman ini semakin nyata mengingat lanskap digital Indonesia yang terus meluas seiring dengan tingginya penetrasi internet nasional (Kartiko, 2025). Sayangnya, masifnya transformasi digital ini belum sepenuhnya diimbangi dengan arsitektur keamanan siber yang komprehensif (Ejjami, 2024). Rentetan insiden kebocoran data strategis nasional dan kelumpuhan sistem pada beberapa institusi pemerintah dalam beberapa tahun terakhir menjadi bukti empiris bahwa Infrastruktur Informasi Vital (IIV) Indonesia masih rentan terhadap infiltrasi (Tommy & Nasution, 2025). Dalam skenario peperangan asimetris, kerentanan pada sektor sipil dan pemerintahan ini dapat dieksploitasi oleh musuh atau proksi asing sebagai pintu masuk untuk melakukan sabotase, memicu instabilitas sosial,

hingga mengunci fungsi-fungsi vital negara sesaat sebelum eskalasi militer terjadi. Hal ini menegaskan bahwa garis batas antara infrastruktur pertahanan militer dan infrastruktur sipil kini semakin kabur, karena keduanya terhubung dalam satu ekosistem jaringan yang sama (Coveri et al., 2024).

Meskipun pemerintah Indonesia telah memiliki instansi seperti Badan Siber dan Sandi Negara (BSSN) yang bertugas menjaga keamanan siber secara umum, ranah penangkalan dan penindakan terhadap ancaman siber yang berdimensi militer dan mengancam kedaulatan negara tetap menjadi domain utama dan tanggung jawab pertahanan Tentara Nasional Indonesia (TNI). Saat ini, wacana pembentukan Angkatan Siber sebagai matra keempat guna melengkapi TNI AD, AL, dan AU semakin kuat disuarakan. Namun, cetak biru operasional, kesiapan sumber daya manusia, serta adaptasi doktrin taktisnya masih memerlukan kajian akademis yang mendalam. Beberapa penelitian terdahulu umumnya berfokus pada kebijakan tata kelola keamanan siber nasional secara makro, namun masih sangat minim literatur yang secara spesifik membedah strategi militer Indonesia dalam merespons ancaman *asymmetric cyber warfare* dari sudut pandang operasi pertahanan aktif.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif-analitis. Pendekatan ini dipilih karena objek kajian yakni strategi pertahanan militer dalam menghadapi *asymmetric cyber warfare* memerlukan pemahaman yang mendalam mengenai doktrin, kebijakan strategis, dan fenomena ancaman siber kontemporer yang tidak dapat diukur semata-mata dengan angka. Metode utama yang digunakan adalah studi kepustakaan atau penelusuran literatur untuk membedah konsep peperangan asimetris di ruang siber dan kesiapan postur pertahanan militer Indonesia.

Data yang digunakan dalam penelitian ini sepenuhnya bertumpu pada data sekunder yang dikumpulkan melalui penelusuran dokumentasi dan pangkalan data akademis. Sumber datanya mencakup dokumen kebijakan pertahanan negara, doktrin Tentara Nasional Indonesia (TNI), regulasi pemerintah terkait keamanan siber (BSSN), hingga literatur akademis dan studi kasus serangan siber global. Penelusuran literatur difokuskan menggunakan kata kunci seperti *"asymmetric warfare", "cyber defense strategy",* dan "Sistem Pertahanan dan Keamanan Rakyat Semesta", yang kemudian diseleksi secara ketat berdasarkan relevansi, kredibilitas, dan kemutakhiran (terbitan 5-10 tahun terakhir).

Proses analisis data menggunakan teknik analisis konten secara interaktif. Langkah-langkah analisis meliputi reduksi data untuk memilah informasi krusial mengenai kerentanan siber dan strategi pertahanan, penyajian data secara naratif dan sistematis, hingga penarikan kesimpulan. Data yang telah direduksi kemudian dianalisis menggunakan pisau bedah konsep Sistem Pertahanan dan Keamanan Rakyat Semesta untuk merumuskan suatu cetak biru strategi pertahanan aktif yang adaptif bagi militer Indonesia di era digital.

HASIL DAN PEMBAHASAN

Anatomi dan Eskalasi Ancaman Asymmetric Cyber Warfare

Dalam peperangan asimetris di ruang siber, ancaman tidak lagi

dimonopoli oleh militer reguler dari negara musuh. Aktor ancaman kini sangat terdesentralisasi, memiliki tingkat anonimitas tinggi, dan mampu melancarkan serangan berskala destruktif dengan biaya operasional yang sangat rendah dibandingkan pengadaan alutsista konvensional. Berdasarkan penelusuran literatur dan analisis insiden global, karakteristik aktor ancaman siber asimetris yang mengancam keamanan nasional dapat diklasifikasikan pada Tabel 1.

Tabel 1. Kategorisasi Aktor Ancaman *Asymmetric Cyber Warfare*

Kategori Aktor	Karakteristik & Kapabilitas	Target Utama	Dampak Asimetris
Sponsored Hackers (APT)	Didanai negara asing, kapabilitas sangat tinggi, operasi jangka panjang dan senyap *(stealthy)*	Rahasia negara, instalasi militer, infrastruktur nuklir/energi (misal: Stuxnet)	Kelumpuhan fungsi negara strategis, pencurian intelijen tingkat tinggi.
Cyber Terrorists	Berideologi ekstrem, kapabilitas menengah hingga tinggi, bertujuan menebar teror massal.	Fasilitas publik, jaringan transportasi, rumah sakit, bursa efek.	Instabilitas sosial, kepanikan massal, dan disrupsi ekonomi skala nasional.
Hacktivists	Bergerak berdasarkan motif politik/sosial, operasi sering berupa *defacement* atau DDoS.	Situs web pemerintah, lembaga penegak hukum, militer.	Penurunan kredibilitas negara dan gangguan layanan publik (psikologis).
Cyber Mercenaries (Proksi)	Tentara bayaran digital, disewa untuk melakukan sabotase tanpa atribusi langsung ke negara penyewa.	Infrastruktur Informasi Vital (IIV), jaringan komando militer (C2).	Sulitnya proses atribusi hukum/militer yang memicu keraguan dalam eskalasi balasan.

Tabel 1 menegaskan bahwa paradigma ancaman yang dihadapi oleh Tentara Nasional Indonesia (TNI) telah berevolusi secara radikal. Dalam skenario peperangan modern, postur pertahanan negara tidak lagi cukup hanya disiagakan untuk menghalau intrusi kinetik dari pasukan berseragam militer di wilayah perbatasan geografis. Sebaliknya, garis depan pertempuran kini telah bergeser ke ruang nirkontak, di mana instrumen penyerangnya berwujud barisan kode berbahaya (*malware*, *ransomware*, maupun *wiper*) yang dirancang secara spesifik untuk menyabotase sistem komando militer dan melumpuhkan infrastruktur vital. Serangan asimetris ini dieksekusi secara terorkestrasi oleh aktor-aktor tak kasat mata baik itu kelompok *state-sponsored hackers* maupun proksi bayaran—yang beroperasi dalam bayang-bayang anonimitas dari jarak ribuan kilometer lintas benua. Kondisi ini menciptakan tantangan atribusi yang sangat kompleks bagi intelijen pertahanan, di mana sebuah invasi destruktif berskala masif dapat terjadi kapan saja tanpa didahului

oleh deklarasi perang formal. Oleh karena itu, TNI dituntut untuk memiliki kapabilitas deteksi dini (*early warning system*) dan mitigasi *real-time* yang melampaui batasan doktrin pertahanan tradisional.

Evaluasi Doktrin dan Kesiapan Postur Pertahanan Militer Indonesia

Hingga saat ini, rancang bangun doktrin pertahanan militer Indonesia secara historis masih sangat berpusat pada proyeksi kekuatan kinetik di tiga matra konvensional (Darat, Laut, dan Udara). Meskipun Tentara Nasional Indonesia (TNI) telah beradaptasi dengan membentuk Satuan Siber (Satsiber TNI), arsitektur operasional dan kedudukannya masih lebih banyak difungsikan sebagai elemen pendukung. Kapabilitas satuan ini umumnya masih terfokus pada fungsi dukungan komando, perlindungan jaringan internal militer, dan pengamanan informasi taktis. Artinya, postur yang ada belum sepenuhnya diproyeksikan sebagai kekuatan tempur pemukul utama (main strike force) yang mampu merancang dan mengeksekusi operasi siber ofensif (Offensive Cyber Operations) berskala masif guna melumpuhkan ancaman dari luar secara proaktif.

Paradigma yang memosisikan ruang siber sekadar sebagai domain pendukung ini melahirkan kelemahan berupa penerapan doktrin pertahanan pasif. Dalam peperangan asimetris digital, respons yang reaktif terhadap *shadow strikes* (serangan bayangan berupa injeksi malware atau penyadapan intelijen) adalah sebuah kerugian taktis yang fatal. Mengingat kecepatan rambat ancaman di ruang siber terjadi dalam hitungan milidetik, doktrin pertahanan yang menunggu infrastruktur vital diserang hingga dampaknya terasa sama artinya dengan menerima kekalahan sebelum pertempuran fisik benar-benar dimulai.

Lebih jauh lagi, ketidakhadiran matra siber (Angkatan Siber) yang berdiri sendiri secara otonom menciptakan ruang hampa dalam rantai komando penindakan pertahanan. Ketika terjadi intrusi spionase siber atau sabotase infrastruktur strategis oleh proksi asing, militer seringkali terbentur oleh batasan yurisdiksi penegakan hukum sipil. Penanganan insiden siber berskala nasional saat ini masih terfragmentasi dan lebih banyak dititikberatkan pada lembaga non-militer. Tanpa adanya otoritas komando setingkat matra yang secara khusus memegang mandat operasi pertahanan negara di ruang siber, respons balasan (retaliation) dari TNI berpotensi menjadi birokratis, kurang agresif, dan pada akhirnya mengurangi daya tangkal (deterrence effect) Indonesia di mata negara kawasan.

Formulasi Strategi Pertahanan Siber Aktif Berbasis Sishankamrata

Untuk membalikkan kerentanan menjadi kekuatan, militer Indonesia perlu mengadopsi doktrin *Active Cyber Defense* yang diintegrasikan dengan filosofi Sistem Pertahanan dan Keamanan Rakyat Semesta (Sishankamrata). Ruang siber yang mayoritas infrastrukturnya (seperti kabel fiber optik, satelit, dan server) dimiliki oleh pihak sipil/swasta, menuntut peleburan batas antara pertahanan militer dan pertahanan sipil. Strategi yang diformulasikan dalam kajian ini mengusulkan model Kolaborasi *Pentahelix* Pertahanan Siber, sebagaimana diilustrasikan pada Tabel 2.

Tabel 2. Matriks Implementasi Sishankamrata di Ruang Siber *(Digital Pentahelix)*

Komponen Sishankamrata	Peran Strategis dalam Operasi Siber	Bentuk Implementasi Aktif
TNI (Komponen Utama)	Penangkalan, penindakan *(offensive cyber ops)*, dan pelindungan instalasi militer.	Pembentukan Angkatan Siber (Matra Ke-4), operasi intelijen siber militer lintas negara.
Pemerintah (BSSN, Kominfo)	Regulasi, tata kelola, dan diplomasi siber internasional.	Pembuatan protokol krisis siber nasional dan penguatan sandi negara.
Industri / Swasta (Komponen Pendukung)	Penyediaan dan pengamanan Infrastruktur Informasi Vital (ISP, Perbankan, Energi).	Berbagi intelijen ancaman *(Threat Intelligence Sharing)* secara *real-time* dengan militer.
Akademisi & Peneliti	Riset, pengembangan teknologi kriptografi, forensik digital, dan kurikulum pertahanan.	Kolaborasi riset dengan Universitas Pertahanan / Akmil untuk rekayasa balik *(reverse engineering)* malware.
Masyarakat & Komunitas IT (Komponen Cadangan)	Kewaspadaan digital, komponen cadangan siber (Pasukan Siber Rakyat).	Mobilisasi komunitas peretas *(white hat hackers)* dan penggiat OSINT sipil saat negara dalam keadaan darurat perang.

Berdasarkan pemetaan struktural pada Tabel 2, arsitektur strategi pertahanan militer di ruang siber bertransformasi secara fundamental, operasi pertahanan tidak dapat lagi berjalan secara eksklusif atau terisolasi dari sektor non-militer. Pendekatan ini menuntut integrasi seluruh elemen kekuatan nasional. Dalam ekosistem pertahanan ini, Komponen Utama yakni Tentara Nasional Indonesia (TNI) diproyeksikan secara mutlak sebagai ujung tombak yang memegang otoritas penindakan terhadap ancaman siber berintensitas tinggi. Kapabilitas ini mencakup netralisasi serangan dari *state-sponsored hackers* (peretas yang didanai negara asing), kontra-spionase digital tingkat lanjut, serta pelaksanaan operasi siber ofensif terukur guna menindak tegas setiap pelanggaran kedaulatan di ruang nirkontak.

Di sisi lain, lapisan pertahanan yang diisi oleh entitas sipil dan sektor swasta khususnya para pengelola Infrastruktur Informasi Vital (IIV) seperti penyedia layanan internet, energi, dan perbankan beralih fungsi menjadi *buffer zone* yang sangat strategis. Lapisan ini bertindak sebagai jaringan sensor peringatan dini yang secara proaktif mendeteksi anomali lalu lintas data dan membagikan intelijen ancaman secara *real-time* kepada komando militer sebelum sebuah serangan mencapai eskalasi kritis. Sinergi lintas sektoral yang terorkestrasi inilah yang merepresentasikan wujud nyata dan adaptasi paripurna dari doktrin Sistem Pertahanan dan Keamanan Rakyat Semesta (Sishankamrata) di medan perang dimensi kelima.

SIMPULAN

Berdasarkan analisis yang telah diuraikan, penelitian ini menarik tiga

kesimpulan utama. Pertama, ancaman *asymmetric cyber warfare* telah meredefinisi konsep peperangan modern, di mana aktor non-negara dan proksi asing dapat mendisrupsi infrastruktur kritis dan stabilitas keamanan nasional Indonesia dari jarak jauh tanpa kontak fisik. Kedua, postur dan doktrin pertahanan militer Indonesia saat ini yang masih berpusat pada kekuatan kinetik dan menempatkan elemen siber sekadar sebagai fungsi pendukung dinilai tidak lagi memadai untuk merespons serangan siber berskala masif yang menuntut kecepatan mitigasi *real-time*. Ketiadaan matra khusus siber menciptakan ruang hampa dalam rantai komando penindakan yang agresif. Ketiga, untuk menghadapi ancaman nirkontak ini, TNI harus bertransformasi dengan mengadopsi doktrin *Active Cyber Defense*. Strategi ini wajib diintegrasikan dengan filosofi Sistem Pertahanan dan Keamanan Rakyat Semesta melalui skema kolaborasi *pentahelix*, di mana militer bertindak sebagai ujung tombak penindakan, sementara sektor sipil dan swasta berfungsi sebagai sistem peringatan dini dan ruang penyangga.

SARAN

Guna memperkuat kedaulatan digital dan ketahanan nasional Republik Indonesia, kajian ini merekomendasikan langkah-langkah strategis berikut kepada para pembuat kebijakan pertahanan.

Percepatan Pembentukan Matra Siber

Pemerintah dan Markas Besar TNI perlu segera merealisasikan pembentukan Angkatan Siber sebagai matra keempat yang mandiri dan otonom. Matra ini harus dibekali wewenang penuh untuk merancang operasi pertahanan dan serangan siber balasan *(offensive cyber operations)* guna menciptakan *deterrence effect* di kawasan.

Harmonisasi Regulasi dan Yurisdiksi

Perlu adanya pembaruan Undang-Undang Pertahanan Negara yang secara eksplisit mengatur batas yurisdiksi dan mandat operasi militer di ruang siber, sehingga TNI memiliki payung hukum yang jelas saat harus mengambil alih kendali krisis ketika infrastruktur vital sipil diserang oleh entitas asing.

Peningkatan Sinergi Intelijen Sipil-Militer

Mendorong pembentukan protokol berbagi intelijen ancaman *(Threat Intelligence Sharing)* secara *real-time* antara institusi militer (BAIS TNI/Angkatan Siber) dengan Badan Siber dan Sandi Negara (BSSN), penyedia layanan internet (ISP), serta akademisi, guna memetakan profil ancaman secara holistik.

DAFTAR PUSTAKA

Budi, E., Wira, D., & Infantono, A. (2021). Strategies For Strengthening Cyber Security To Achieve National Security in Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia*, *3*(November), 24–25. https://doi.org/10.54706/senastindo.v3.2021.141

Christello, G. (2025). *The rise of Iran's cyber capabilities and the threat to us critical infrastructure*. *12*(1), 12–22.

Coveri, A., Cozza, C., & Guarascio, D. (2024). Blurring Boundaries: An Analysis of the Digital Platforms-Military Nexus. *Review of Political Economy*, 1–32. https://doi.org/10.1080/09538259.2024.2395832

Ejjami, R. (2024). The Digital Evolution Strategies for Overcoming Cybersecurity and Adoption Challenges in French SMEs. *International Journal for Multidisciplinary Research*, *6*(3), 1–25.

Heller, K. J. (2021). *In Defense of Pure Sovereignty in Cyberspace In Defense of Pure Sovereignty in Cyberspace*. *97*.

Kartiko, A. (2025). *Intelijen Keamanan dan Politik Identitas: Mengawal Demokrasi (Strategi Intelligence-Led Policing pada Pemilu 2014 dan 2019)*. USK Press.

Khan, Z. F. (2025). Cyber Warfare and International Security: A New Geopolitical Frontier Dr. *The Critical Review of Social Sciences Studies Online*, *3*(2), 513–527.

Prasetyo, F. C., Gumilar, R. N., & Prihantoro, M. (2026). *Pengembangan Doktrin Perang Berlarut dalam Rangka Sistem Pertahanan Negara di Era Modern*. 493–505.

Sharma, L. (2025). *Warfare Without Borders: An era of Asymmetric and Cyber Warfare*. *II*(I), 42–52.

Tarom, M. (2025). THE STRATEGIC ROLE OF DEFENSE EDUCATION IN STRENGTHIENING INDONESIA'S NATIONAL SECURITY SYSTEM. *Jurnal Pendidikan Dan Pengembangan Sumber Daya Pertahanan*, *2*(1).

Tommy, S., & Nasution, M. I. P. (2025). EVALUASI MANAJEMEN RISIKO KEAMANAN SIBER PADA INFRASTRUKTUR DIGITAL PEMERINTAH : STUDI KASUS PUSAT DATA NASIONAL (PDN). *Jurnal Manajemen Ekonomi Dan Bisnis (JMEB)*, *04*(01), 1–26.

Yu, A., Kolotylo, I., Hashim, H. A., & Eltoukhy, A. E. E. (2025). Electronic Warfare Cyberattacks , Countermeasures , and Modern Defensive Strategies of UAV Avionics : A Survey. *IEEE Access*, *13*(March), 68660–68681. https://doi.org/10.1109/ACCESS.2025.3561068