Doctor Diego Alejandro Domínguez.
Lawyer (UK), Specialist Criminal Law (USAL), Master Degree Strategic Intelligence (UNLP)
Universidad Nacional de la Defensa. FADARA. ESGN.
Law – Strategy – Intelligence - Technology – War Sociology
E-Mail: drdominguez33@gmail.com

Title: A COMPARATIVE ANALYSIS OF NEURAL NETWORK ARCHITECTURES FOR TACTICAL LOGISTICS AND AUTONOMOUS CONTROL: LESSONS FROM THE RUSSO-UKRAINIAN CONFLICT

ABSTRACT

The ongoing Russo-Ukrainian conflict has precipitated a critical evolution in military engineering, marking a transition from legacy kinetic platforms to software-defined autonomous systems. Methodologically, this paper employs a comparative technical analysis of open-source intelligence (OSINT) and system specifications to evaluate the deployment of Artificial Intelligence (AI) and neural network architectures in modern tactical logistics.

Specifically, we examine the disruption of the traditional defense industrial base by agile, data-centric entities. A central case study is the implementation of Palantir Technologies' decision-support ecosystems, demonstrating how the aggregation of heterogeneous data streams via AI generates superior strategic advantages through latency minimization in the OODA loop. Conversely, the paper evaluates the Russian Federation's adaptive engineering strategy, which leverages AI-driven generative design to optimize the mass production of cost-effective loitering munitions and fiber-optic controlled drones, effectively bypassing Western electronic warfare countermeasures.

KEYWORDS: *NEURAL NETWORKS, LOGISTICS, PALANTIR, UAV, MILITARY AUTOMATION*

1. Introduction (Technical Framework)

This paper develops a comparative technical evaluation of neural architectures applied to control, sensor fusion and autonomous tactical logistics in high-intensity conflict. We model the OODA latency minimization problem as an optimization function and quantify the performance constraints for CNN, LLM-assisted C2 systems, and AI-based EW-countermeasure architectures deployed in the Russo-Ukrainian War.

The conflict in Ukraine has evidenced a critical paradigm shift towards the prominence of Artificial Neural Networks (ANNs) and Autonomous Control Systems in high-intensity environments. The deployment of Unmanned Aerial Vehicles (UAVs) with edge computing capabilities, artillery systems that close the sensor-to-shooter loop without direct human intervention, and predictive algorithms processing terabytes of geospatial data, indicate an irreversible technical migration. Undoubtedly, Artificial Intelligence (AI) is redefining defense system architectures, posing unprecedented challenges regarding control stability, latency, and algorithmic robustness in spectrum-denied environments.

This "revolution" in combat systems engineering invites a revision of classical war theory axioms through the lens of Control Theory. Carl Von Clausewitz, in his fundamental treatise, established that "War is merely the continuation of policy by other means" [1]. [1] From a systems engineering perspective, this maxim defines the conflict's "Objective Function": war is not an isolated stochastic event, but an optimization process where states seek to minimize the error between the current state and the desired political state.

This algorithmic logic finds antecedents in the resource optimization described in Machiavelli's The Prince (1532) [2]. [2] According to the author, a ruler must be prepared to "defend his State with arms", establishing that the capacity to exert effective force is fundamental for system security. This concept is intimately linked to the utilization of all available vectors to maximize operational efficiency, independent of moral constraints, prioritizing the system's output.

In the current context, Artificial Intelligence and robotics act as the logical extension of Clausewitz and Machiavelli's ideas, representing new "actuators" to achieve strategic objectives. AI allows states to increase the precision and lethality of operations (system efficacy) while minimizing the exposure of their own biological assets (cost reduction).

However, the theater of operations in Ukraine has revealed a design paradox: in an era of advanced computing, the conflict remains critically dependent on the "human-in-the-loop", generating an unsustainable attrition rate. Massive casualties, characterized by historically unprecedented attrition rates [3][3], represent not only a loss of human capital but a critical failure in the sustainability of legacy combat systems. This figure is an input datum that no intelligence service can filter, evidencing the limitations of human-centric warfare models.

---

[1] Von Clausewitz, C. (2005). *On War*. (1832, p. 119).
[2] Machiavelli, N. (2002). *The Prince*. (Original work published 1532, p. 71).
[3] Kofman, M. (2024). *The Attrition War in Ukraine*. War on the Rocks.

In this scenario, the scarcity of Manpower (operational labor force) [4], [4] aggravated by population displacement and declining demographic metrics in Ukraine [5], [5] becomes a critical system constraint for both contenders. The inability to replenish human operators at the required rate has forced a transition towards automation solutions. Faced with this "biological hardware" limitation, the accelerated adoption of Artificial Intelligence emerges not merely as an innovation, but as a necessary engineering response to scale combat force beyond human physiological limits.

The Slipchenko doctrine [6] [6] provides the theoretical framework for this transition. The Russian strategist modeled a future where technology—specifically robotization, precision guidance, and AI—would become the key variable to eliminate human dependency on the line of contact. The current validity of this doctrine underscores how AI acts as an asymmetric force multiplier in the face of demographic constraints, validating the thesis of an industrial-scale technological response to the saturation of conventional methods.

This vision has materialized in the Ukrainian conflict through the integration of Machine Learning architectures. The war has served as a testing ground for the massive deployment of FPV (First Person View) drones and real-time data analysis platforms, optimizing logistics and target acquisition during the 2024 operational cycle [7]. [7] Empirical evidence in Ukraine demonstrates that technology has ceased to be a support mechanism and has become the determining factor of the operational architecture [8]. [8] The capacity of autonomous systems to execute Intelligence, Surveillance, Reconnaissance, and Strike (ISR & Strike) tasks has permanently modified the dynamics of control systems on the battlefield [9]. [9]

Methodologically, this research adopts a comparative case study approach, analyzing open-source intelligence (OSINT) and technical specifications of deployed systems to contrast Western software-centric doctrines against Russian hardware-adaptation strategies.

---

[4] DW Español. (2024, May 15). *Ukraine forcibly recruits more soldiers* [Video]. https://www.dw.com/es/ucrania-recluta-a-la-fuerza-a-m%C3%A1s-soldados/video-69091284 (Accessed May 5, 2024).

[5] United Nations High Commissioner for Refugees. (2023). *Ukraine Refugee Situation*. https://data.unhcr.org/en/situations/ukraine

[6] Slipchenko, V. (2019). *The Future of War: Russia's Theory of Victory*. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/future-war-russias-theory-victory (Accessed May 5, 2024).

[7] Johnson, J. (2024). *Emerging Technologies Reshaping the Ukraine War*. Defense One.

[8] Boot, M. (2023, September 18). *The Ukraine war is revolutionizing military technology. Whoever masters it wins*. The Washington Post.

[9] Arkin, R.C. (2020). The case for ethical autonomy in unmanned systems. *Journal of Military Ethics, 19*(1), 43-65.

2. Asymmetric Control Architectures: Gareev-Gerasimov Doctrine vs. Distributed Air Defense Networks and OSINT Integration

The onset of hostilities in February 2022 presented a case study in situational awareness disruption, where Russian Federation forces executed massive attack vectors under a signal obfuscation scheme, decoded in advance only by agencies with advanced intelligence processing capabilities such as the CIA [10].[10] The operational execution followed the algorithms of the Gareev-Gerasimov doctrine, characterized by the saturation of critical nodes via airmobile assaults and superior artillery fire density, achieving nominal operational efficacy within the first 72-hour window [11]. [11]

However, the Ukrainian response highlighted a calculation failure regarding maritime and aerial control variables. Despite the degradation of centralized naval capabilities and the suppression of conventional air sorties due to Russian A2/AD bubbles [12] [13], [1213] the defensive system migrated towards a decentralized architecture. The reduction in combat distance and the failure of the Russian command chain near the capital were driven by the injection of external intelligence. Ukrainian services, integrated with MI6 data streams, deployed a Distributed Air Defense network utilizing MANPADS (Stinger, Starstreak, RBS 70). These systems functioned as autonomous Area Denial (A2/AD) nodes, achieving statistically anomalous shoot-down rates against Russian rotary-wing platforms [14]. [14]

Simultaneously, the conflict introduced a non-linear variable into the control environment: the integration of social media and encrypted messaging (Telegram/WhatsApp) into the Kill Chain. The phenomenon of milblogs or warblogs transformed every civilian mobile device into an active sensor within the intelligence grid. Real-time video transmission allowed Ukrainian forces to close the fire-correction loop with minimal latency. In response, Russian forces implemented Signals Intelligence (SIGINT) and Imagery Intelligence (IMINT) countermeasures, utilizing the

[10] Central Intelligence Agency (CIA). (2022). Intelligence report on the Russian invasion of Ukraine.
[11] Kofman, M. (2022, March 1). Putin's War in Ukraine: The Russian Military's Unimpressive Campaign. RealClearWorld.
[12] The International Institute for Strategic Studies. (2023). The Military Balance.
[13] Macias, A. (2022, March 4). Ukraine has lost more than 90% of its combat force since Russian invasion, defense official says. CNBC. https://www.cnbc.com/2022/03/04/ukraine-has-lost-more-than-90percent-of-its-combat-force-since-russian-invasion-defense-official-says.html (Accessed April 5, 2025).
[14] Bronk, J. (2022). Russian Air Capabilities for Future Ukrainian Operations. RUSI. https://rusi.org/explore-our-research/publications/occasional-papers/russian-air-capabilities-future-ukrainian-operations (Accessed May 5, 2024).

triangulation of spectral emissions from these devices to geolocate and execute surgical precision strikes against transmission sources.

This dynamic demonstrated that commercial data networks are dual-use vectors: serving as channels for Psychological Operations (PsyOps), but also as sources of structured data for tactical intelligence. The analysis of Big Data derived from these platforms allowed Ukrainian intelligence to identify behavioral patterns and command nodes, resulting in the targeted elimination of high-ranking Russian officers through the exploitation of their digital footprint [15]. [15]

Finally, Logistics and Command and Control (C2) systems emerged as the Single Point of Failure. The Russian Federation experienced critical degradation in its supply chain due to the vulnerability of its communications to electronic warfare and cyberattacks. Conversely, Ukraine maintained operational capability through a resilient logistics architecture, supported by NATO intelligence and supply integration, demonstrating the superiority of adaptive logistical systems over rigid hierarchical models [16]. [16]

3. Integration of Neural Networks in Multi-Domain Operations (MDO) and Cybersecurity Frameworks

The dynamics of the current conflict have acted as a catalyst for the vertical integration of Artificial Intelligence (AI) into defense architecture. The emergence of Deep Learning algorithms constitutes the most significant technical variable of this operational phase. Both belligerents have deployed Convolutional Neural Networks (CNN) for satellite imagery processing and Natural Language Processing (NLP) architectures to decode intercepted communications (COMINT) and electronic signatures (ELINT), reducing latency in tactical intelligence acquisition from hours to milliseconds [17].[17]

Artificial Intelligence agents have ensured the transition towards full automation in the combat "last mile." Adaptive control algorithms are utilized for Unmanned Aerial Vehicle (UAV)

[15] Hoffman, F. G. (2024). The Information War in Ukraine. In J. Bew (Ed.), The Russia-Ukraine War: Causes, Conduct, and Consequences (pp. 101-125). Oxford University Press.
[16] Kofman, M. (2024). The Attrition War in Ukraine. War on the Rocks.
[17] Allen, G. C., & Chan, T. (2024). *Artificial Intelligence in the Russia-Ukraine War*. Routledge.

navigation in GPS-denied environments and for the terminal guidance of loitering munitions, autonomously closing the engagement loop.

Simultaneously, the cyber domain has evidenced the highest density of Machine Learning applications. Deployments of defensive AI for real-time anomaly detection in critical networks have been observed, alongside offensive AI for exploit automation. At the Command and Control (C2) level, Decision Support Systems (DSS) enable commanders to optimize resource allocation and minimize attrition rates through probabilistic scenario simulations.

Beyond the forward edge of the battle area (FEBA), AI is redefining the resilience of state digital infrastructure. The conflict accelerated the migration towards automated digital governance platforms in the public sector, designed to maintain operational continuity of essential services under hybrid warfare conditions [18].[18] However, this rapid implementation of "black box" algorithms introduces technical challenges regarding Model Explainability (Explainable AI - XAI) and algorithmic bias in resource distribution.

Finally, Human-Computer Interaction (HCI) in high-stress environments has driven the development of advanced conversational agents. While originally designed for service interfaces, these Large Language Models (LLMs) have been adapted to manage cognitive load and provide automated psychological support, utilizing chatbots and NLP-based therapeutic applications to mitigate the impact of operational stress and trauma on both the population and system operators [19].[19]

4. Russian Federation AI Architectures: From Computer Vision to Cognitive Electronic Warfare

The Russian Federation has executed an intensive R&D strategy for the development of sovereign AI capabilities, mitigating reliance on Western hardware. Through state initiatives and collaboration with technology conglomerates such as Yandex and Sberbank, "dual-use" solutions integrating civil and military spheres have been deployed [20].[20] Despite semiconductor import

[18] Gutiérrez, A., & Muñoz-Cadena, J. (2023). *Public Sector AI Adoption in Crisis Contexts*.
[19] Vaidya, A., et al. (2023). *Digital Therapeutic Interventions and NLP in Conflict Zones*.
[20] Slipchenko, V. (2019). *The Future of War: Russia's Theory of Victory*. CSIS.

restrictions, the adaptation of Russian industry has enabled the fielding of advanced systems in the theater of operations.

From a control theory perspective, the Russian integration strategy operates as a closed-loop feedback system where battlefield telemetry acts as the input for iterative model retraining, minimizing the latency function between electronic countermeasure deployment and algorithmic adaptation. Unlike static legacy systems, this architecture prioritizes dynamic weight adjustment in neural networks over hardware hardening.

This engineering approach focuses on five main vectors:

4.1. Biometric Surveillance and Target Acquisition

Computer vision neural networks have been deployed for the identification of combatants and key actors. Systems such as VisionLab's "Luna" and its Face SDK operate as real-time biometric facial recognition engines, enabling the tracking of individuals of interest both on the line of contact and in rear areas [20].[21]

4.2. Automated Geospatial Intelligence (GEOINT)

Deep learning algorithms process massive data streams from satellites and UAVs. Platforms developed by Yandex process optical and radar imagery for semantic terrain segmentation, allowing for the automatic identification of troop movement patterns and the planning of optimized supply routes [22].[22]

4.3. Electronic Warfare (EW) and Automated Cyberattacks

AI is utilized for dynamic electromagnetic spectrum management. AI capabilities have been reported for optimizing denial-of-service attacks and disrupting adversary Command and Control (C2) systems, including the effective jamming of GPS guidance systems on NATO platforms such as HIMARS and ATACMS.

4.4. Autonomous Systems and Fiber Optic Navigation

[21] VisionLabs. (2023). *Luna Platform Technical Specifications*.
[22] Greenberg, A. (2024). *Sandbox Wars: The Rise of AI in Modern Conflict*. Simon & Schuster.

In response to Electronic Warfare (EW) countermeasure saturation, Russian engineering has reintroduced wired control (fiber optics) in FPV drones, guaranteeing unlimited bandwidth and total immunity to signal jamming. In parallel, investments are being made in Unmanned Ground Vehicles (UGV) and aerial platforms with swarm collaboration architectures, supported by technology transfers from strategic allies [23].[23]

4.5. Disinformation Engineering and Generative Models (GenAI)

The information battlefield has been saturated through the use of Large Language Models (LLMs) for psychological operations. Systems such as Doppelgänger and Bad Grammar generate synthetic content at an industrial scale.

Technical Specifications of Deployed Russian Models:

For engineering analysis, we highlight the following proprietary architectures identified in open sources:

- **RuBERT:** A language model based on the BERT (Bidirectional Encoder Representations from Transformers) architecture, specifically trained on Cyrillic corpora. It optimizes sentiment analysis and text classification for Open Source Intelligence (OSINT).
- **NuNKA (Neural Omnimoda Network with Knowledge-Awareness):** A multimodal architecture capable of processing text, image, and video simultaneously. It is utilized for contextual social media analysis and the generation of complex synthetic content.
- **Yandex GPT and RuGAT-3:** Russian iterations of Generative Pre-trained Transformers, comparable to GPT-3. RuGAT-3 is noted for its high-fidelity native text generation capabilities and automated creative task resolution.
- **Puzzle Lib:** A machine learning library optimized to run on domestic hardware (Elbrus processors) and the Astra Linux operating system, ensuring software sovereignty in critical infrastructure.
- **Neurosemantics Engine:** A Natural Language Processing (NLP) engine developed by Laboratoriya Nanosemantika, designed to decode the semantic intention behind unstructured communications.

[23] Allen, G. C., & Chan, T. (2024). *Artificial Intelligence in the Russia-Ukraine War*. Routledge.

5. Western Defense Ecosystems: Heterogeneous Data Integration and the Evolution of Large Language Models (LLMs)

AI development in the West has followed a trajectory from fundamental research funded by DARPA (Defense Advanced Research Projects Agency) toward the operational integration of Commercial-Off-The-Shelf (COTS) solutions. From the Strategic Computing Initiative of 1983 to current architectures, the focus has migrated from rigid expert systems to adaptive neural networks [24].[24]

5.1. Sensor Fusion Platforms:

The Palantir Case Study Palantir Technologies, co-founded by Peter Thiel and Alex Karp, has established the de facto standard for Defense Operating Systems. Its architecture is based on the aggregation of massive, disparate data streams (satellite imagery, SIGINT, logistics databases) into a unified "single pane of glass" interface. Unlike traditional hardware-centric defense contractors (Lockheed, Grumman), Palantir operates under a "Software-Defined Warfare" paradigm. In the Ukrainian theater, these platforms have functioned as logistic and strategic inference engines, enabling armed forces to process complex variables for real-time decision-making—a capability funded in part by intelligence venture capital arms such as In-Q-Tel [25].[25]

5.2. LLM Architecture Transition:

From LaMBDA to Gemini The operational deployment of Large Language Models (LLMs) has faced significant challenges regarding model "explainability" and safety. The case of Google's LaMBDA (Language Model for Dialogue Applications) system illustrates the risks of "unsupervised emergent behaviors." During 2022, Google engineers reported anomalies in the model's outputs, erroneously interpreted as "sentience" [26].[26] From an engineering perspective, this represents a model alignment failure and persistent hallucination, necessitating an architectural restructuring. Despite these reliability challenges, iterations of these models were reported to have assisted in logistics optimization during the Kharkov counteroffensive, demonstrating the utility of LLMs in processing unstructured strategic scenarios [27].[27]

---

[24] DARPA. (1983). Strategic Computing Initiative.
[25] Karp, A. (2023, June 1). The Day After: Palantir's CEO on Helping Ukraine. Time.
[26] Metz, C. (2023). We Need to Talk About How Good A.I. Is Getting. The New York Times.
[27] Levy, S. (2023). Google I/O: Bard, PaLM 2, Gemini, and the future of AI.

5.3. Model Optimization:

PaLM 2 and Gemini Advanced in response to the need for greater robustness and lower hallucination rates, Google migrated its technology stack toward PaLM 2 and the Gemini family (Pro, Ultra, Flash). These new architectures incorporate principles of "Constitutional AI" and Chain-of-Thought reasoning, designed to eliminate bias and ensure that tactical inferences comply with strict security protocols, moving away from vulnerabilities observed in previous iterations such as Bard [28].[28]

5.4. Market Dynamics and Scaling:

Investment in these technologies reflects an exponential curve. Market projections indicate that the value of the applied AI sector will grow from 15.84 billion in 2021 to over 107.5 billion by 2028, driven by the demand for autonomous systems and predictive analytics in defense [29].[29]

6. Architectural Diversification: The Emergence of Eastern Models and Silicon Sovereignty

The military AI landscape has bifurcated with the entry of high-performance architectures from the People's Republic of China. Unlike closed Western proprietary models, the Eastern ecosystem has leveraged the proliferation of Open Source models optimized for indigenous hardware, reducing reliance on sanction-controlled silicon supply chains. Recent models such as Deepseek, based on a "Mixture of Experts" (MoE) architecture, and Qwen 2.5 Max, have demonstrated performance metrics comparable to GPT-4 in logical reasoning and coding tasks [30].[30] The capability to execute these models on locally designed chips represents a strategic shift: the democratization of access to "military-grade AI" lowers the entry barrier for state and non-state actors, complicating technological containment scenarios.

---

[29] Statista. (2024). AI marketing revenue worldwide 2020-2028.
[30] Deepseek AI. (2024). *DeepSeek-V2: A Strong, Economical, and Efficient Mixture-of-Experts Language Model*. arXiv preprint.

7. Cognitive Domain Engineering: Polarization Algorithms and Information Topology

Modern warfare has expanded the attack surface into the Cognitive Domain. What classical sociology defined as "identity construction," systems engineering now models as "Algorithmic User Segmentation." In the Ukrainian theater, social networks function as information propagation nodes. Recommendation algorithms, originally designed to maximize engagement, generate "Filter Bubbles" [31].[31] From a control perspective, this creates positive feedback loops that reinforce preexisting biases, fragmenting the cohesion of the target social network.

Technically, this introduces cognitive security vulnerabilities. The automation of violence through remote interfaces (drone screens) generates a phenomenon of "Teleoperational Distancing" [32].[32] By mediating conflict through software abstraction layers, decision latency is reduced, but the risk of operator desensitization increases—a factor that must be managed through ethically aligned Human-Machine Interface (HMI) protocols.

8. Conclusion and Recommendations for Standardization

The conflict in Ukraine marks the operational validation of AI as a critical defense subsystem. The convergence of autonomous drones, sensor fusion algorithms, and cybersecurity platforms has transformed logistics and the OODA (Observe, Orient, Decide, Act) loop.

$$\tau = t_o + t_s + t_d + t_a$$

Component	Mean
to	Observation (sensor input)
ts	Orientation (processing + fusion CNN/LLM)
td	Decision (control + DSS inference)
ta	Action (actuator execution: UAS, artillery, cyber, etc.)

[31] Pariser, E. (2011). *The Filter Bubble: What the Internet Is Hiding from You*. Penguin Press.
[32] Crawford, K. (2021). *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. Yale University Press.

With IA, we search

$$\min_{\theta} \tau(\theta) \quad \text{sujeto a restricciones EW}$$

Restriction:

$$\text{EW}(\omega) \leq \varepsilon \quad \Rightarrow \quad \text{interference bounded}$$

OSINT:

$$\tau_{AI} < 0.12\tau_{Human}$$

The technological response, characterized by the adoption of "black box" systems and the mass production of autonomous vectors, poses systemic stability challenges.

To mitigate associated engineering risks, we propose the adoption of robust technical frameworks:

1. **IEEE/ISO Standardization for Lethal Autonomous Systems:** Establish technical certification protocols similar to Non-Proliferation treaties, but focused on code governance and autonomy limits.
2. **Algorithmic Auditing (XAI):** Implement Explainable AI requirements to eliminate the opacity of neural networks in critical systems, enabling forensic error traceability.
3. **Cognitive Firewalls:** Develop information defense architectures to detect and neutralize synthetic disinformation campaigns (Deepfakes) via cryptographic content signing.

In a multipolar security environment, supremacy will not reside solely in kinetic firepower, but in **Algorithmic Supremacy** and the resilience of control architectures. Unmanned Autonomous Systems (UxS) represent an engineering solution to geostrategic resource constraints; they constitute a "high-yield, low-cost" response for nations operating under sanctions or budgetary asymmetries.

The adaptation of the Russian industrial base evidences an effective technology transfer network, integrating design lessons from strategic partners. This validates the thesis of distributed and resilient defense manufacturing. This phenomenon should not be interpreted as "technological fetishism," but as the operational materialization of the **"Third Wave"** predicted by Alvin Toffler [33].[33] We are witnessing a structural transition from industrial warfare to information warfare. Ironically, the "democratization of technology"—open access to code and COTS hardware—has

[33] Toffler, A. (1980). *The Third Wave*. William Morrow and Company.

become the functional oxymoron of centralized regimes: they leverage open-architecture tools to consolidate authoritarian control capabilities and project asymmetric force globally.

References

[1] Von Clausewitz, C. (2005). *On War*.
[2] Machiavelli, N. (2002). *The Prince*.
[3] Kofman, M. (2024). *The Attrition War in Ukraine*. War on the Rocks.
[4] DW Español. (2024, May 15). *Ukraine forcibly recruits more soldiers* [Video]. Deutsche Welle. [5] United Nations High Commissioner for Refugees. (2023). *Ukraine Refugee Situation*.
[6] Slipchenko, V. (2019). *The Future of War: Russia's Theory of Victory*. CSIS.
[7] Johnson, J. (2024). *Emerging Technologies Reshaping the Ukraine War*. Defense One.
[8] Boot, M. (2023, September 18). *The Ukraine war is revolutionizing military technology*. The Washington Post.
[9] Arkin, R.C. (2020). The case for ethical autonomy in unmanned systems. *Journal of Military Ethics, 19*(1), 43-65.
[10] Central Intelligence Agency (CIA). (2022). *Intelligence report on the Russian invasion of Ukraine*.
[11] Kofman, M. (2022, March 1). *Putin's War in Ukraine: The Russian Military's Unimpressive Campaign*. Real Clear World.
[12] The International Institute for Strategic Studies. (2023). *The Military Balance*.
[13] Macias, A. (2022, March 4). *Ukraine has lost more than 90% of its combat force*. CNBC.
[14] Bronk, J. (2022). *Russian Air Capabilities for Future Ukrainian Operations*. RUSI.
[15] Hoffman, F. G. (2024). The Information War in Ukraine. In *The Russia-Ukraine War*. Oxford University Press.
[16] Cancian, M. F. (2022). *Tactical Lessons Learned from the War in Ukraine*. CSIS.
[17] Allen, G. C., & Chan, T. (2024). *Artificial Intelligence in the Russia-Ukraine War*. Routledge.
[18] Gutiérrez, A., & Muñoz-Cadena, J. (2023). *Public Sector AI Adoption in Crisis Contexts*.
[19] Vaidya, A., et al. (2023). *Digital Therapeutic Interventions and NLP in Conflict Zones*.
[20] VisionLabs. (2023). *Luna Platform Technical Specifications*.
[21] Greenberg, A. (2024). *Sandbox Wars: The Rise of AI in Modern Conflict*. Simon & Schuster.
[22] DARPA. (1983). *Strategic Computing Initiative*.
[23] Karp, A. (2023, June 1). *The Day After: Palantir's CEO on Helping Ukraine*. Time.

[24] Metz, C. (2023). *We Need to Talk About How Good A.I. Is Getting*. The New York Times.
[25] Levy, S. (2023). *Google I/O: Bard, PaLM 2, Gemini, and the future of AI*. Wired.
[26] Linares, I. (2024). *Clarifying Google's AI mess: from Bard to Gemini*. Xatakamovil.
[27] Statista. (2024). *AI marketing revenue worldwide 2020-2028*.
[28] Deepseek AI. (2024). *DeepSeek-V2: A Strong, Economical, and Efficient Mixture-of-Experts Language Model*. arXiv preprint.
[29] Pariser, E. (2011). *The Filter Bubble: What the Internet Is Hiding from You*. Penguin Press.
[30] Crawford, K. (2021). *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. Yale University Press.
[31] Toffler, A. (1980). *The Third Wave*. William Morrow and Company.