**AI-POWERED TACTICAL INTELLIGENCE IN**

**MILITARY OPERATIONS**

**ABSTRACT**

In modern military operations, rapid and accurate decision-making is critical for maintaining situational awareness and operational superiority. Traditional intelligence methods rely heavily on manual analysis of visual data, which is time-consuming and inadequate for the fast-paced nature of contemporary warfare. To address these limitations, this project presents an AI-Powered Tactical Intelligence System that leverages machine learning and deep learning to automate the classification of military assets such as tanks, helicopters, airplanes, and artillery units, enabling faster and more reliable battlefield assessments.

The system processes image data through a comprehensive pipeline involving resizing, normalization, and compression to ensure high-quality input for model training. It employs multiple classification models, including a Perceptron for baseline evaluation, a Deep Neural Network (DNN) for non-linear pattern recognition, and a hybrid CNN-RNN (Convolutional Neural Network with LSTM) architecture designed to capture both spatial features and contextual dependencies in imagery. The dataset is split into training and testing sets to ensure robust evaluation, and all models are trained and saved for reuse.

Performance is evaluated using key metrics such as accuracy, precision, recall, F1-score, sensitivity, and specificity. Results show that the CNN-RNN model significantly outperforms traditional methods by effectively learning hierarchical visual features, leading to superior classification accuracy. A confusion matrix and classification report provide detailed insights into model behaviour, while heatmaps and performance graphs enhance interpretability.

A user-friendly Tkinter-based GUI enables seamless interaction through two distinct modes: ADMIN mode for dataset management, preprocessing, and model training; and USER mode for real-time image classification and visualization of training accuracy and loss curves. By integrating advanced AI techniques into a practical framework, the system demonstrates the potential of data-driven intelligence to enhance threat recognition and decision support in dynamic military environments.

* **KEYWORDS**: - AI-Powered Tactical Intelligence, Military Asset Classification, Convolutional Neural Network (CNN), Recurrent Neural Network (RNN/LSTM), Deep Neural Network (DNN), Perceptron Classifier, Image Preprocessing, Situational Awareness, Tkinter GUI, Accuracy and Loss Visualization, Model Evaluation Metrics, Automated Threat Recognition, Hybrid CNN-RNN Architecture, Real Time Decision Support.

**CHAPTER 1**

**INTRODUCTION**

**1.1 Introduction**

Artificial Intelligence (AI) is revolutionizing military intelligence by enabling faster, more accurate, and adaptive decision-making in increasingly complex and data-intensive battlefields. Traditional intelligence methods are struggling to cope with the vast amounts of multisource data generated from satellites, drones, sensors, and cyber networks. AI systems overcome these limitations by processing information at machine speed, using machine learning, computer vision, and natural language processing to detect threats, predict enemy behaviour, and recommend actions. This enhances situational awareness, accelerates response times, and improves mission effectiveness across all domains—land, sea, air, space, and cyberspace. AI also supports autonomous systems, cyber defence, electronic warfare, and strategic planning through simulations, reducing the cognitive load on human analysts and allowing them to focus on higher-order decision-making.



**Fig 1.1: AI in Military Operations**

Despite its transformative potential, the integration of AI into military operations presents significant ethical, strategic, and operational challenges. Concerns include the use of lethal autonomous weapons, accountability for AI-driven decisions, algorithmic bias, and the risk of unintended escalation. Overreliance on AI may lead to automation bias, while adversarial attacks and disinformation can undermine system reliability. Moreover, an emerging global AI arms race threatens strategic stability and lowers the threshold for conflict. To address these risks, robust governance, international cooperation, transparency (such as through Explainable AI), and human oversight are essential. The future of military AI depends not only on technological advancement but also on responsible development and deployment to ensure ethical integrity, strategic stability, and long-term security.

**1.2 RESEARCH MOTIVATION**

Modern wars generate huge amounts of data from drones, satellites, radars, and sensors. Human analysts cannot process all this information quickly, which often causes delays in making decisions. This creates the need for a system that can handle large data, analyze it in real-time, and support commanders in taking faster actions. Artificial Intelligence (AI) provides this ability by using machine learning and data-driven models to detect patterns, predict threats, and give timely intelligence. Another motivation is that today’s battlefields are very dynamic and unpredictable. Traditional intelligence methods are slow and rigid, which makes them less effective against new types of threats like cyberattacks, terrorism, and hybrid warfare. AI-powered systems can continuously learn from past and present data, adapt to changing situations, and suggest the best possible decisions. This adaptability makes AI very useful in modern tactical operations.AI also reduces the workload on human soldiers and officers. In a war situation, too much information can overwhelm decision-makers. With AI handling repetitive and time-consuming analysis, military leaders can focus on critical decisions and planning. This teamwork between humans and AI improves both speed and accuracy. Finally, AI-powered tactical intelligence helps in reducing risks and improving mission success. It supports precise targeting, better resource allocation, and early threat detection, which decreases chances of errors and unnecessary losses. Using explainable AI also makes the decisions transparent and reliable. For these reasons, research in AI for tactical intelligence is highly motivated, as it can transform modern defence systems into smarter, faster, and safer operations.

**1.3 PROBLEM DEFINATION**

Modern military operations generate massive and rapidly growing volumes of data from sensors, surveillance systems, communication channels, and digital intelligence sources. This data overload often exceeds the capacity of human analysts, leading to delays in fusing information, identifying threats, and making informed tactical decisions. The reliance on manual analysis not only slows response times but also increases the risk of overlooked patterns or critical intelligence. Additionally, frontline tactical units often lack advanced predictive tools that could provide real-time, automated insights to enhance situational awareness. These gaps highlight the urgent need for AI-powered systems capable of synthesizing complex data streams, enabling faster, more accurate, and proactive decision-making in dynamic operational environments. Building on this, the exponential growth of battlefield information—ranging from real-time sensor feeds and geospatial data to intercepted communications and social media monitoring—has created significant challenges for military personnel tasked with operational analysis. The sheer volume and velocity of incoming data routinely overwhelm conventional computational and human resources, resulting in cognitive bottlenecks and delayed situational understanding. As tactical missions become increasingly complex and time-sensitive, traditional manual data processing methods are insufficient, causing critical intelligence to be missed or delivered too late to influence operational outcomes. Tactical units often operate without robust predictive analytics, leaving them reactive rather than anticipative in fast-evolving scenarios. This deficit underlines the necessity for integrated, automated intelligence platforms driven by artificial intelligence—systems robust enough to continuously synthesize multi-domain data sources, instantly highlight emerging threats or opportunities, and deliver actionable recommendations in real-time, directly addressing the limitations of current manual and fragmented analytical approaches

**1.4 SIGNIFICANCE**

The study on AI-powered tactical intelligence is highly significant because it addresses the growing need for faster and more accurate decision-making in modern warfare. Military operations today generate massive amounts of data from drones, satellites, sensors, and cyber systems, which are difficult for humans to analyze quickly. By introducing Artificial Intelligence into tactical intelligence, this study helps in transforming raw data into meaningful insights that can guide commanders in real-time. The research is also important because it reduces the risks faced by soldiers on the battlefield. With AI predicting enemy movements, detecting threats early, and suggesting the best course of action, military forces can avoid unnecessary losses and increase mission success rates. This ensures not only safety for troops but also greater efficiency in resource use and operational planning. Another key significance lies in the adaptability of AI systems. Traditional intelligence methods are rigid and slow, while AI can continuously learn and adjust to new threats like cyberattacks or asymmetric warfare. This makes the study highly relevant for modern defence strategies that demand flexibility and speed. Finally, the study contributes to building trust in AI systems by focusing on explainable and transparent decision-making. Commanders can understand why a decision or prediction was made, which increases confidence in using AI as a support tool. Overall, this research is significant as it combines human expertise with machine intelligence to create a powerful decision-support system for safer, smarter, and more effective military operations.

**1.5 RESEARCH OBJECTIVES**

1. To build an AI-driven tactical intelligence framework that can integrate data from multiple sources such as drones, satellites, ground sensors, and communication networks.

2. To design data preprocessing and fusion techniques for cleaning, filtering, and combining raw military data to make it suitable for AI models.

3. To develop machine learning and deep learning algorithms capable of real-time threat detection, enemy tracking, and situation assessment.

4. To apply predictive analytics for forecasting enemy strategies, resource requirements, and possible outcomes of different tactical decisions.

5. To create an adaptive decision support system that can learn continuously from past operations and improve its intelligence over time.

6. To reduce the workload of human commanders by automating routine analysis tasks, allowing them to focus on high-level planning and mission-critical judgments.

7. To ensure accuracy and precision in tactical operations\* through optimized resource allocation, better mission planning, and reduced collateral damage.

8. To integrate Explainable AI (XAI) so that the system’s predictions and recommendations are transparent, trustworthy, and easy to understand for human operators.

9. To evaluate the system’s effectiveness under different simulated battlefield scenarios to test its speed, accuracy, adaptability, and reliability.

10. To contribute towards safer and smarter military operations by combining human intelligence with AI support for faster, data-driven decision-making.

**1.6 APPLICATIONS**

1. **Autonomous Mission Planning:** DRL optimizes strategies and suggests best tactical maneuvers.
2. **Cybersecurity Defence:** Detects adversarial attacks, spoofing, or data manipulation in real time.
3. **Electronic Warfare:** AI helps in detecting, analyzing, and jamming enemy signals.
4. **Logistics & Supply Chain Management:** Predicts equipment failures and ensures timely resource delivery.
5. **Search & Rescue Operations:** AI-powered systems locate soldiers or civilians in disaster or conflict zones.

**1.7 ADVANTAGES**

1. **Faster Decision-Making**: Processes battlefield data in real time, enabling quicker and more accurate responses.
2. **Improved Situational Awareness**: Fuses inputs from drones, satellites, sensors, and communications for a complete battlefield picture.
3. **Reduced Human Workload**: Automates data analysis, lowering cognitive burden on commanders and soldiers.
4. **Risk Reduction**: Deploys unmanned systems (drones, robots) for dangerous missions, minimizing human exposure
5. **Decision Support for Commanders**: Provides real-time recommendations, reducing decision delays

**CHAPTER 2**

**LITERATURE SURVEY**

**Tan, Y., et.al (2013)[1]** provide a comprehensive review of swarm robotics research up to 2013, synthesizing algorithmic advances, hardware trends, and theoretical foundations that enable large-scale collective behaviour. The paper categorizes core swarm behaviours—such as aggregation, flocking, foraging, and collective decision-making—and maps each to the underlying control laws and bio-inspired mechanisms researchers have used. It highlights distributed control strategies that emphasize local sensing and communication and contrasts them with centralized approaches in terms of scalability and robustness. Important algorithmic themes covered include consensus, potential fields, and probabilistic/stochastic methods for emergent behavior. The authors discuss hardware constraints common in swarm platforms (limited computation, sensing, energy) and how algorithm design compensates for these limitations. They also examine metrics for swarm performance and resilience, noting a need for standardized benchmarks. Applications surveyed range from environmental monitoring to search-and-rescue, with discussion on how realism in simulation affects transfer to real robots.

**Sharkey, N. (2016) [2]** examines the ethical and control-architecture implications of keeping humans “in the loop” for weapon systems, arguing that supervisory control is both a moral and operationally necessary design principle. The chapter frames different modes of human involvement—in the loop, on the loop, out of the loop—and analyzes their impact on responsibility, situational awareness, and error management. Sharkey critiques architectures that excessively automate lethal decisions, stressing that meaningful human control must include not only approval authority but also comprehension of AI decision processes. The discussion integrates human factors literature to show how operator workload, automation bias, and trust calibration affect supervisory performance. There is emphasis on the technological prerequisites for effective supervision: transparent system behaviour, interpretable outputs, and predictable failure modes. Sharkey also highlights legal and policy constraints, suggesting design principles to align system autonomy with International Humanitarian Law.

**Kott, A., et al. (2018) [3]** propose a structured reference architecture for Autonomous Intelligent Cyber-defence Agents (AICA), aiming to formalize how intelligent agents can autonomously detect, analyze, and respond to cyber threats in tactical environments. The architecture delineates modules for sensing, decision-making, planning, learning, and execution, emphasizing modularity so agents can be tailored to platform-specific constraints. A key contribution is the integration of adaptive learning components with safety constraints, allowing agents to refine responses while bounding risk through policy and human-in-the-loop overrides. The paper discusses the importance of robust threat models and adversarial reasoning to anticipate sophisticated attacks, especially in contested networks. Communication and coordination protocols for multi-agent cyber defence—necessary for distributed military networks—are detailed, with attention to bandwidth and latency limitations typical in operational settings.

**Alexander Kott et al. (2018) [4]** in this follow-up release refine the original AICA blueprint with expanded design guidance, implementation notes, and more rigorous treatment of agent lifecycle management. Release 2.0 digs deeper into learning safeguards, describing how continual learning can be governed to prevent model drift and unintended behaviours in the field. It adds more explicit interface specifications for interoperability between heterogeneous agents and with human operators, which is crucial for combined human–agent cyber defence operations. The updated document strengthens sections on threat attribution and decision provenance, recognizing the need for explainability in cyber response actions that have operational consequences. There is added emphasis on red-team evaluation frameworks, adversarial machine learning resilience, and integration with enterprise-level security orchestration.

**Akhtar, N., et.al (2018) [5]** provide a systematic survey of adversarial examples in computer vision, cataloguing attack types (white-box, black-box), perturbation strategies, and the threat they pose to deep neural nets used for perception tasks. The paper summarizes metrics used to evaluate adversarial effectiveness and transferability, showing how small, often imperceptible perturbations can drastically change model outputs. It also reviews defence mechanisms—adversarial training, input preprocessing, detection heuristics—and critically appraises their limitations, especially against adaptive attackers. The survey emphasizes the practical implications for safety-critical systems (autonomous vehicles, surveillance), noting that robustness in research benchmarks often does not translate to field resilience. The authors discuss theoretical explanations for vulnerability, including high-dimensional geometry and linearity in deep networks, and note open problems in certifiable robustness. There is a valuable section on evaluation methodology, urging standardized protocols for comparing defences.

**Biggio, B., et.al (2018) [6]** reflect on a decade of adversarial machine learning research, tracing its evolution from theoretical proofs-of-concept to more mature, practically oriented attack–defence cycles. They synthesize advances in poisoning attacks (training data manipulation) and evasion attacks (runtime input manipulation), and discuss the shifting focus from purely academic threat models to ones that consider attacker goals and constraints. The paper examines defence trends, including robust optimization and game-theoretic formulations, and argues for security evaluations that account for adaptive adversaries. A recurring theme is the arms-race nature of the field: defences provoke stronger attacks, which then motivate new defences. The authors advocate for security-oriented machine learning that integrates adversary-aware design, formal guarantees, and real-world testing. They also note cross-cutting challenges like interpretability and benchmark standardization. For domains such as military decision support, the survey offers a cautionary lesson—model performance metrics must be complemented by adversarial robustness assessments to ensure trustworthiness in contested environments.

**Jovanoska, et.al (2018) [7]** present methods for fusing heterogeneous sensor data to improve detection and tracking of small unmanned aerial vehicles (UAVs), an increasingly important capability for defence and airspace security. The paper compares classical fusion schemes—centralized, decentralized, and hybrid—and demonstrates how combining radar, acoustic, optical, and RF sensors produces more robust detection under clutter and low-observable conditions. They detail signal processing pipelines and association algorithms that manage disparate sampling rates and sensor accuracies. A notable contribution is discussion of track-level fusion strategies that maintain identity and kinematic consistency across sensor types. The authors address practical issues such as false-alarm management, occlusion handling for optical sensors, and RF signal intermittency.

**Dosilović, et.al (2018) [8]** provide a survey on explainable artificial intelligence (XAI), reiterating and extending previous work with additional applied examples and practical considerations for deploying explanations. The paper stresses the importance of aligning explanation granularity with the user’s role—operators, commanders, or analysts—and suggests modular explanation architectures that can serve different stakeholders. It provides a succinct taxonomy of explanation types (global vs. local, model-specific vs. model-agnostic) and discusses case studies where explanations improved system acceptance or enabled error discovery. The authors also highlight computational trade-offs: some explanation techniques are costly and unsuitable for low-latency contexts.

**Cummings, M. L. (2019) [9]** interrogates the concept of “meaningful human control” over lethal autonomous weapons, contrasting normative expectations with operational realities of system certification and deployment. She introduces the notion of “meaningful human certification,” the formal processes, tests, and standards that verify a system’s behaviour and constraints before fielding, and argues that certification complements, but does not replace, human-in-the-loop ethics. The paper discusses human cognitive limitations in supervising complex autonomous systems, and questions whether human oversight can realistically prevent unintended harm at machine timescales.

**Preece, et.al (2019) [10]** explore how Explainable AI can be leveraged to augment human intelligence in complex multi-domain operations (land, sea, air, space, cyber). The paper argues that XAI enables more effective human–AI teaming by providing understandable rationales for recommendations in time-sensitive contexts. It presents architectures for integrating explanation modules into decision-support pipelines, emphasizing real-time constraints and the need for concise, actionable explanations for commanders. The authors consider cross-domain data fusion challenges and how explanations can help reconcile conflicting evidence from heterogeneous sources. They also discuss evaluation frameworks that measure not only explanation fidelity but operational utility—for example, whether explanations improve decision speed and accuracy.

**Johnson, M., et.al (2019) [11]** advocate viewing AI not as isolated automation but as teammates integrated into collaborative decision-making structures. Drawing from human–computer interaction and organizational behaviour, the authors outline principles for designing AI systems that communicate intent, negotiate tasks, and adapt to team norms. They identify key capabilities required for AI teammates: transparency, predictability, shared mental models, and the ability to explain actions. Experimental and theoretical findings show systems designed for teaming produce better joint performance than black-box tools. The paper also explores socio-technical aspects of trust calibration, role assignment, and responsibility distribution within mixed human–AI teams. They argue for iterative co-design with end-users and emphasize the importance of social cues (timing, phrasing) in AI communication.

**Sisson, M. (2019) [12]** examines how AI can be applied to reduce risks associated with autonomous defense systems, blending technical assessment with policy implications. The report analyzes risk categories—operational failure, accidental escalation, adversarial exploitation—and maps AI techniques that can mitigate each. It highlights rigorous testing, simulation, and constrained autonomy as practical mitigations, and proposes layered safeguards including human oversight and fail-safe behaviours. Transparency and certification processes to ensure reliability and legal compliance are stressed. Scenario-based analyses illustrate how risk reduction strategies function under varying threat environments and communication constraints. Sisson also discusses trade-offs between operational effectiveness and conservative design choices prioritizing safety.

**Clinciu, M.-A., et.al (2019) [13]** provide a concise mapping of terminology in the explainable AI community, addressing inconsistent usage hurdling research comparability and practitioner uptake. The survey catalogs terms such as interpretability, explainability, transparency, and accountability, clarifying subtle distinctions and common overlaps. It advocates for standardized definitions and proposes a taxonomy organizing explanation objectives (debugging, legal compliance, user trust) against explanation methods (feature attribution, symbolic rules, example-based explanations). The authors highlight evaluation challenges, noting that different stakeholders demand distinct explanation properties. By systematizing language, the paper aims to reduce confusion in multidisciplinary teams and enable clearer communication between developers, domain experts, and regulators. This terminological clarity is particularly beneficial in defence applications where precise contractual and legal language matters.

**Tjoa, E., et.al (2019) [14]** survey XAI with a focus on medical applications, drawing lessons transferable to safety-critical domains such as military decision support. They review interpretable model classes, post-hoc explanation techniques, and evaluation methodologies tailored for clinical settings where trust and liability are paramount. They discuss how domain knowledge can be encoded into interpretable structures to improve performance and user acceptance. The authors stress the importance of causal explanations in medicine—an insight emphasizing explanation types useful for diagnosis and treatment decisions. They critique common explanation metrics that ignore user comprehension and call for human-subject evaluations. The survey highlights regulatory drivers (e.g., explainability requirements in healthcare) and how pressures shape research priorities.

**Yaacoub et al., (2020) [15]** review multipurpose military drone applications across ISR, logistics, EW, and precision strike. They map mission profiles to platform classes, sensors, and autonomy levels. The survey discusses swarming and collaborative perception. Communications resilience covers anti-jam, LPI/LPD, and SATCOM fallback. Edge AI enables on-board detection and tracking at low latency. Counter-UAS threats prompt stealth and hardening measures. The authors weigh ethical and legal constraints on targeting, and highlight operational gaps including endurance, contested C2, and weather robustness. They underscore test/validation needs for complex airspace, guiding capability planning.

**Morgan et al., (2020) [16]** analyze ethical concerns in uncertain military AI deployments, highlighting accountability gaps, bias, and escalation risk. “Meaningful human control” is operationalized through governance and training. They discuss assurance evidence including testing, audits, and red-teaming. They consider dual-use dynamics and proliferation pressures, proposing transparency norms and coalition coordination. Risk mitigations include bounded autonomy and fallback modes. Data governance and privacy are covered for multinational operations. The report urges scenario-based evaluations under stress and offers a framework for ethical readiness.

**Fernández-Villacañas Marín, (2021) [17]** argues for integrated modelling and simulation beyond standalone simulators. The paper critiques gaps in human-factors realism and adversary behaviours and proposes digital twins and live-virtual-constructive blends. Data pipelines should close the loop from exercises to model updates. Validation under uncertainty is prioritized, and procurement must reward modularity and openness. The author highlights analytics for training transfer and readiness metrics. Scenarios should include degraded communications and EW effects. Collaborative standards enable cross-platform reuse. The vision reframes modelling and simulation as an ecosystem.

**Agarwala, (2021) [18]** surveys AI-powered vision in modern munitions enabling autonomous/semi-autonomous targeting. Core tasks include detection, classification, and tracking in clutter. Compute and power constraints drive model compression and edge inference. The paper covers sensor fusion (EO/IR/SAR) for robustness. It addresses IHL compliance, confidence thresholds, and human-on-the-loop control. Adversarial robustness and countermeasures are analyzed, and environmental factors such as weather, smoke, and occlusion are treated systematically. The author discusses testing with high-fidelity simulations and ranges. Safety interlocks and no-fire zones are considered. The study maps research to fieldability.

**Raja Soundaran et al., (2021) [19]** propose a machine learning-based volatile blockchain to secure routing in military sensor networks. Volatility minimizes on-chain states while preserving trust. Machine learning predicts stable, secure routes under mobility and jamming. The design resists Sybil, blackhole, and wormhole attacks. Experiments measure throughput, latency, and energy, showing better resilience than classic protocols. Lightweight cryptography enables constrained devices. The paper discusses key management and fault recovery. Scalability to large, dynamic topologies is analyzed, outlining deployment on edge gateways.

**Andrijašević et al., (2021) [20]** present a broad survey of quantum technologies for defence applications. Quantum sensing promises superior detection and navigation in GPS-denied settings. Quantum key distribution (QKD) supports secure communications against future adversaries. The paper catalogs Technology Readiness Levels (TRLs) and timelines for subsystems. Hybrid classical–quantum workflows offer near-term gains. Practical issues include cryogenics, stability, and calibration. Standards and interoperability are nascent but needed. The authors assess threat and benefit asymmetries, recommending targeted pilots and dual-use pathways. The survey frames realistic adoption horizons.

**Rizzi et al., (2021) [21]** review computational fluid dynamics (CFD) progress for separated flows relevant to military aircraft. They cover turbulence modelling and hybrid RANS-LES approaches. Mesh adaptation and wall modelling are detailed. Validation uses wind-tunnel and flight datasets. Uncertainty quantification informs design margins. Applications include high-angle-of-attack control and stores release. The paper shows CFD guiding envelope expansion and discusses coupling with control-law development. Remaining gaps involve massively separated, transient phenomena. Recommendations target HPC scaling and data-driven surrogates.

**O’Neill et al., (2021) [22]** provide a systematic review of human–autonomy teaming evidence. Benefits arise with clear role allocation and transparency. Pitfalls include automation bias and overtrust. The authors recommend adaptive autonomy and shared mental models. Metrics span performance, trust, and workload. They highlight team-level training and debrief practices. Interface design should expose system intent and limits. Communication bandwidth and latency affect teaming fluency. Longitudinal field studies beyond lab demos are needed. The review guides human-autonomy teaming program design.

**Dongyuan et al., (2022) [23]** propose a method learning aerial combat maneuvers using confrontation demonstrations plus dynamic quality replay. Imitation seeds the policy; prioritized replay stabilizes reinforcement learning. Shaped rewards balance survivability, energy, and positional advantage. Curriculum training and domain randomization improve robustness. Evaluations show higher win rates and tactic diversity. Ablations assess replay quality and opponent variety. Policies generalize to unseen adversaries in simulation. The method addresses sparse and unstable rewards common in air combat. Transfer pathways to higher-fidelity environments and safety constraints for real-world applicability are discussed.

**Galán et al., (2022) [24]** map the research landscape of military machine learning using bibliometrics to reveal growth trajectories, collaboration networks, and influential venues. They identify dominant clusters including computer vision for ISR, autonomous platforms, cyber defence, and C2 analytics, while noting underexplored areas such as explainable AI and assurance. Co-authorship and country-level analyses show evolving multinational partnerships tied to funding ecosystems. Keyword co-occurrence charts expose shifts from handcrafted features to deep learning and from static datasets to streaming data. Citation bursts highlight seminal works anchoring robustness and adversarial machine learning. The study surfaces methodological gaps such as scarce standardized benchmarks, limited open datasets, and fragmented evaluation metrics. Recommendations include longitudinal datasets, replicable pipelines, and cross-domain transfer studies. Policy implications focus on targeted funding for safety, simulation-to-field transfer, and human–AI teaming. The paper provides a meta-view prioritizing impactful research directions.

**Gupta et al., (2022) [25]** design an embedded-friendly pipeline for detecting military vehicles from UAV feeds, focusing on constrained compute and energy budgets. A compact convolutional neural network (CNN) backbone is pruned and quantized to meet edge latency while preserving accuracy. The dataset is augmented for small targets, motion blur, and oblique viewpoints, reflecting realistic flight profiles. Experiments vary altitude, ground sample distance, and lighting to test robustness, with onboard inference benchmarks against Jetson-class systems on chips. Post-processing tracks detections temporally to stabilize outputs and reduce false positives. The approach compares favourably to heavier detectors, achieving real-time performance. Thermal and power envelopes are profiled for sustained sorties. The authors discuss communication-aware designs that transmit metadata instead of raw frames. Limitations include domain shift across terrains and sensors. They propose continual learning at the edge with secure model updates.

**Kornberger et al., (2022) [26]** reconceptualize strategy as engagement, drawing parallels to military command philosophies like mission command. They argue effective strategy emerges from iterative interaction with dynamic environments rather than fixed plans. Narrative and identity shape collective action, complementing analytics and key performance indicators. The authors stress distributed decision rights, local initiative, and learning loops under uncertainty. Case insights illustrate how framing and sensemaking influence maneuver choices. They connect these ideas to modern multi-domain operations, where tempo and ambiguity dominate. Practical takeaways include pre-commitment to principles, not scripts; maintaining optionality; and cultivating strategic empathy. The paper invites leaders to balance doctrine with adaptability and warns against over-reliance on dashboards that suppress weak signals. The lens is useful for AI-enabled, fast-changing battlefields.

**Sousa et al., (2022) [27]** survey the interplay of video games and AI, spanning procedural content generation, opponent modelling, and human–AI interaction. They review benchmarks that catalyzed reinforcement learning progress and discuss simulation-to-real insights for training autonomy. Serious games emerge as cost-effective venues for military decision skills, after-action review, and stress inoculation. The authors emphasize data logging and analytics for measuring learning outcomes. They highlight co-creative tools where AI assists instructors to tailor difficulty and narrative. Transfer learning, curriculum design, and domain randomization are presented as bridges to field conditions. Ethical considerations include data privacy and manipulative design patterns. Standardizing interfaces and telemetry improves reproducibility. The paper advocates open environments to accelerate research while maintaining operational relevance.

**Asher et al., (2022) [28]** explore reinforcement learning for strategic maneuver and disruption in multi-agent coordination tasks. They formalize adversarial objectives that pressure policies into robustness against deception and partial observability. Communication constraints are modelled to reflect electromagnetic-contested settings, prompting emergent implicit coordination. Results show policies discovering flanking, feints, and resource denial strategies. The study dissects credit assignment and scalability via decentralized training with centralized critics. Safety envelopes and rules of engagement are encoded as constraints. Ablations trace the impact of opponent diversity and curriculum. The authors advocate standardized scenarios for comparability and outline interpretability hooks to surface intent and rationale during operations.

**Tadić et al., (2022) [29]** propose a multi-sensor approach for UAV detection and 3D localization, fusing radar with electro-optical and infrared cues. Tracking filters such as extended and unscented Kalman filters handle intermittent observations and clutter. The system models kinematics under low signal-to-noise ratio and variable aspect angles, improving detection probability. Calibration and time synchronization receive detailed treatment to reduce fusion bias. The method manages occlusion and background confusion, enhancing track continuity. Evaluation spans range, altitude, and clutter regimes, with receiver operating characteristic analyses for false-alarm control. The architecture supports distributed sensors for perimeter defence. Compute footprints and communication bandwidth are profiled for real-time deployment. The authors note resilience to evasive trajectories and low-radar cross-section drones. Future work includes adding acoustic and radio frequency signatures.

**Jovanoska et al., (2022) [30]** extend multi-sensor fusion for UAV detection to robust 3D localization using heterogeneous data streams. They develop association strategies to disambiguate targets amid clutter and decoys. Filter design considers latency differences and measurement noise across modalities. Field-like tests show tighter confidence ellipsoids and fewer track swaps. The system supports handoff between wide-area radar and narrow field-of-view electro-optical sensors. Real-time considerations include asynchronous buffering and GPU-accelerated kernels. False alarms are reduced through context-aware gating. The approach is positioned for critical infrastructure protection. Limitations include sensitivity to calibration drift. The authors propose auto-calibration using over-the-horizon trajectories.

**Kotyan, (2023) [31]** surveys adversarial machine learning with a focus on vision-specific attack and defence dynamics. Attacks range from evasion, poisoning, backdoors, model extraction, to physical-world patches. Defences include adversarial training, certified robustness, preprocessing, and anomaly detection. The survey critiques evaluation practices susceptible to gradient masking and weak threat models. Transferability and query efficiency are analyzed across architectures and datasets. The author emphasizes the physical realizability of attacks relevant to defence imagery. Robustness auditing and standardized leaderboards are recommended. Open problems involve adaptive attackers, distribution shifts, and real-time constraints. The work helps operational teams prioritize defence-in-depth.

**Eker et al., (2023) [32]** study how simulation variety influences deep-learning detectors of military vehicles. By diversifying weather, terrain, sensor models, and camera poses, they test generalization beyond narrow domains. Results show broader variety reduces overfitting and improves robustness to edge cases but can dilute specificity without curriculum structure. The paper introduces metrics for coverage of rare conditions and performs ablation on fidelity versus performance. Domain randomization is balanced with photorealism to avoid uncanny artifacts. The team profiles training costs and data curation time. Transfer to limited real images shows measurable gains. Recommendations include hybrid pipelines mixing synthetic and curated real data.

**King et al., (2023) [33]** evaluate immersive simulation for specialty military medical training, quantifying skill retention and decision speed. They discuss scenario realism, casualty modelling, and stress inoculation with controlled exposure. Virtual reality-enabled debrief tools provide objective performance analytics and heatmaps of attention. Findings indicate improved triage accuracy and procedural adherence. The study addresses simulator sickness, accessibility, and instructor workload. Cost-benefit analyses favour blended programs combining VR with live exercises. Ethical concerns around psychological safety and data privacy are surfaced. Curricula design emphasizes progressive complexity. The work guides procurement and pedagogy for military medicine.

**Lew et al., (2023) [34]** integrate physics simulation, deep-learning surrogates, and experiments to design architected materials. Inverse design frameworks search vast configuration spaces for targeted stiffness, strength, or damping. Uncertainty quantification prioritizes which candidates to fabricate and test. Validation closes the loop, improving surrogate fidelity iteratively. Demonstrations include lattices with exceptional strength-to-weight ratios. The authors discuss scaling to manufacturing and variability control. They propose data standards for reproducibility and knowledge transfer. Defence implications include lightweight protective structures and resilient components. Limitations involve multi-physics coupling and real-world loading conditions. The approach accelerates materials discovery under constraints.

**Harris et al., (2023) [35]** assess VR for decision training, measuring situation awareness, cognitive load, and transfer to tabletop and live tasks. VR enables safe repetition of rare, high-stress scenarios with controlled variables. Instructor dashboards support formative feedback and objective metrics. Participants show improved engagement and faster observe-orient-decide-act cycles. The study notes team-coordination dynamics and communication protocols within VR. Accessibility and hardware fit are discussed for diverse trainees. The authors suggest integrating AI-driven adversaries and scenario generators. Privacy and data governance are emphasized for recorded sessions. The work supports scalable decision readiness training.

**Lee et al., (2023) [36]** propose a “Deep-AI military staff” to fuse heterogeneous intelligence for cooperative battlefield situation awareness. Multi-agent models coordinate to recommend actions under communication constraints. Explanatory summaries surface rationale, uncertainty, and alternatives for commanders. Benchmarks test detection completeness, tempo, and resilience to sensor loss. The system integrates with command and control workflows and human approval gates. Simulations show improved mission outcomes through coordinated recommendations. The authors analyze trust calibration via explanation granularity and consistency. They address adversarial deception and data poisoning safeguards. Scalability and modular interfaces support coalition operations. The study bridges AI analytics with doctrinal decision-making.

**Hussen et al., (2023) [37]** present a streaming cybersecurity framework using optimized deep learning for big-data environments. Feature engineering is paired with scalable model serving to sustain throughput under attack surges. The pipeline tunes thresholds dynamically to manage false alarms. Evaluation tracks detection latency, recall, and resource consumption. The authors address model drift and online retraining safeguards. They consider privacy and compliance for cross-domain data flows. Deployment guidance includes containerization and observability. Results indicate robust performance against mixed attack types. The approach supports security operations centers defending high-tempo, mission-critical networks. Future work targets federated learning and adversarial robustness.

**Gaire, (2023) [38]** offers an accessible overview of military AI across sensing, autonomy, cyber, logistics, and command and control. Benefits include speed, precision, and scalability; risks span bias, brittleness, and escalation. The review underscores human–machine teaming as a doctrine shift, not just tooling. Explainability and audit trails are positioned as enablers of trust and accountability. National strategies and investment patterns are summarized with regional contrasts. The paper calls for standard test ranges, synthetic data pipelines, and red-teaming. It highlights legal and ethical debates around lethal autonomy. Education and workforce upskilling are emphasized. The piece serves as a primer for policymakers and practitioners.

**Rej et al., (2023) [39]** analyze the dynamic relationships among terrorism, military expenditure, and tourism in India using autoregressive distributed lag models. They examine both short-run shocks and long-run equilibria with structural-break awareness. Findings suggest nuanced interactions that inform policy on security spending and economic stability. The study addresses endogeneity, stationarity, and diagnostic checks. It emphasizes careful interpretation to avoid spurious causality claims. Implications include calibrated investment in security to safeguard tourism flows. Limitations include data quality and model sensitivity. The work illustrates econometric tools for security–economy trade-offs and encourages richer datasets and robustness tests.

**Regal et al., (2023) [40]** review virtual reality training for chemical, biological, radiological, and nuclear response, where live training is hazardous and costly. They discuss scenario realism—agent dispersal, personal protective equipment constraints, and sensor behaviour—within virtual environments. The paper highlights psychological safety, workload management, and instructor control. Interoperability with live drills and tabletop exercises is encouraged for transfer. Metrics focus on procedural correctness, timing, and coordination. Technical challenges include haptics for donning/doffing and respiratory load simulation. The authors propose modular scenario libraries and competency frameworks. Data privacy and ethical use guidelines are outlined. The study charts a roadmap for scalable, safe CBRN preparedness.

**Meerveld et al., (2023) [41]** argue that refraining from military AI adoption can be ethically irresponsible when it reduces harm and improves protection. They balance innovation duty with compliance to international humanitarian law. The paper promotes governance structures, transparency, and audit trails to align AI use with legal norms. It warns against capability overreach and unchecked autonomy. Case reasoning suggests contexts where AI decreases collateral damage via precision and foresight. Human competence and training remain central to safe deployment. The authors advocate evidence-based policy and ongoing evaluation. They call for international dialogue on norms and verification. The piece reframes the ethics debate toward responsible utilization.

**Bestiuk, (2023) [42]** explores the integration of natural language AI for military decision support and swarm control in autonomous unmanned aerial systems. The study leverages combat simulation environments to train AI agents capable of interpreting human commands in plain language. This enables real-time, dynamic coordination among UAS swarms for reconnaissance, targeting, and defensive operations. The system translates natural language into executable mission parameters, significantly reducing operator cognitive load. Bestiuk demonstrates that embedding language models within the control loop improves operational flexibility and speed. The work also addresses adversarial robustness, showing how trained models can adapt to unpredictable battlefield scenarios. Simulation trials reveal increased swarm survivability and mission success rates compared to purely manual or scripted control. The author suggests future integration with multi-modal inputs such as visual and sensor data to enhance situational awareness.

**Reddit Discussion, (2023) [43]** compiles an online community discussion tracing the historical evolution of autonomous weapons platforms, featuring insights from military historians, technologists, and AI researchers. Contributors outline key technological milestones, from early remote-controlled devices to AI-powered autonomous drones and ground vehicles. The timeline includes notable deployments, international treaties, and controversial incidents involving semi-autonomous systems. Users debate ethical, legal, and strategic implications of growing autonomy in warfare. While anecdotal, the discussion aggregates diverse expert opinions, making it a valuable informal knowledge base. It highlights the acceleration of AI integration post-2015 and the role of open-source technologies in military innovation. The thread also touches on geopolitical competition, where leading nations are racing toward fully autonomous combat capabilities. This resource reflects real-time public perception and professional speculation about the future trajectory of autonomous weapon systems.

**King et.al (2023) [44]** examine the application of immersive simulation technologies in developing military general practitioners. The paper describes how virtual environments and realistic combat scenarios can enhance medical decision-making skills under stress. Using VR-based platforms, trainees interact with AI-driven patients exhibiting complex trauma conditions. The study demonstrates improvements in diagnostic speed, treatment prioritization, and procedural accuracy after immersive training. The authors highlight the importance of realism in simulation to build resilience and situational adaptability. They also discuss the scalability of such training systems for mass deployment across military medical units. Limitations include hardware cost and potential technology acceptance barriers among older personnel. Overall, the research underscores the transformative potential of immersive simulation for preparing military medical staff for high-pressure combat environments.

**Raio et al., (2023) [45]** investigate reinforcement learning as a pathway toward autonomous, intelligent cyber-defence agents for vehicle platforms. Their approach models vehicle network security as a dynamic adversarial environment, where RL agents learn to detect, mitigate, and recover from cyber threats. The system is trained in simulated networks to recognize anomalous traffic patterns, malware signatures, and intrusion attempts. The authors propose a multi-agent configuration for distributed defence, enabling vehicles to share threat intelligence in real time. Experimental results show reduced attack success rates and faster recovery compared to traditional rule-based intrusion detection systems. The study also explores transfer learning to adapt trained agents to different vehicle architectures. The authors highlight the importance of explainability and robustness against adversarial machine learning attacks in defence contexts.

**Carrasco-Davis et al., (2023) [46]** survey reinforcement learning applications in swarm robotics, highlighting algorithms suited for multi-agent coordination in dynamic environments. They classify RL techniques into model-free, model-based, and hybrid approaches for swarm control. They emphasize decentralized learning, where individual agents adapt locally while contributing to collective intelligence. Applications span search-and-rescue, environmental monitoring, and military surveillance. The review analyzes challenges like sparse rewards, non-stationarity, and scalability in large swarms. Algorithmic trends such as multi-agent deep RL and policy sharing are examined. The authors compare performance metrics like adaptability, convergence speed, and robustness. They also address the trade-offs between training in simulation and real-world deployment. Case studies include UAV swarms for reconnaissance and UGV teams for mine detection. Future work calls for explainable RL policies and cross-domain transfer learning. Ethical implications of autonomous swarms in defence contexts are discussed.

**Jingyu et al., (2023) [47]** apply deep reinforcement learning to master an air combat simulation game, integrating flight dynamics and tactical decision-making. They present a multi-layered framework combining high-level strategy and low-level control. Actor–critic methods are used for maneuver planning in a continuous action space. The simulation environment models realistic combat physics, including missile kinematics and situational awareness constraints. A reward shaping technique accelerates learning by emphasizing kill probability and survival time. Comparative experiments show the DRL agent outperforming scripted and rule-based opponents. The paper addresses computational efficiency via parallel training and curriculum learning. Transferability to real-world UAV combat is discussed, emphasizing sensor noise handling. The results suggest DRL’s potential in complex, adversarial, and high-speed scenarios. The authors note the importance of human–AI teaming for operational safety.

**Fabuyi, (2024) [48]** investigates synthetic data as a means to mitigate bias in AI model training, with defence applications in mind. Synthetic datasets are generated to balance underrepresented classes and combat skewed distributions. The study outlines techniques like GANs, simulation environments, and rule-based data synthesis. Experimental validation shows bias reduction in classification accuracy across demographic groups. The work also discusses regulatory compliance for military AI systems using synthetic data. Advantages include reduced data collection costs and privacy protection. Limitations involve the risk of overfitting to synthetic artifacts. The author presents case studies in facial recognition and target classification. The framework is proposed as a guideline for ethical AI model development. Future research calls for hybrid datasets combining real and synthetic samples for improved generalization.

**Henderson, (2024) [49]** explores explainable AI (XAI) in military contexts, focusing on transparency for decision-critical systems. The author categorizes XAI methods into post-hoc explanations, interpretable models, and interactive visualization tools. Military-specific challenges include time-sensitive operations and classified data handling. The paper uses examples from threat assessment, mission planning, and autonomous targeting. Henderson argues that interpretability must balance operational secrecy and accountability. Techniques like saliency maps, SHAP values, and counterfactual reasoning are discussed. The author emphasizes human–AI trust as a determinant of adoption. Case studies illustrate XAI integration into command-and-control dashboards. Policy recommendations address ethical and legal requirements under international humanitarian law. The study concludes that explainability should be embedded during AI system design rather than as an afterthought.

**Hussen et al., (2024) [50]** present a real-time drone detection system leveraging the Gray Level Co-occurrence Matrix (GLCM) for texture analysis. A graphical user interface (GUI) is developed for field usability. The system processes live video feeds, extracting GLCM features for machine learning classification. Test scenarios include detecting drones against varied backgrounds and lighting. Accuracy is validated using confusion matrices and ROC curves. The authors note resilience against partial occlusion and small target sizes. The GUI provides instant alerts and target tracking visualization. Applications extend to military base defence and event security. Computational efficiency allows deployment on portable hardware. The study proposes integrating radar and acoustic sensors for improved robustness.

**Tanwar et al., (2024) [51]** review the integration of Augmented Reality (AR), Virtual Reality (VR), and haptic feedback technologies in military training. The authors discuss how these immersive tools enhance realism in combat simulations, improving decision-making under stress. They highlight the benefits of haptics in creating tactile feedback for weapons handling and medical procedures. The study compares AR/VR training with traditional methods, emphasizing cost-effectiveness and safety. Technological challenges such as latency, resolution, and motion sickness are addressed. The paper categorizes use cases into tactical drills, equipment familiarization, and mission rehearsal. AR is noted for overlaying battlefield data, while VR provides fully synthetic environments for scenario-based training. Haptics bridge sensory gaps, fostering muscle memory and operational readiness. The review also considers psychological resilience building through simulated high-pressure situations. The authors conclude with research gaps in interoperability and multi-user training environments. They call for AI integration to personalize training pathways.

**Lundberg et al., (2024) [52]** focus on designing Command and Control (C2) systems as systems-of-systems (SoS). The authors analyze how complex military operations require interoperability among heterogeneous subsystems. They propose an architecture framework facilitating modularity, scalability, and resilience. Case studies from NATO exercises illustrate real-world SoS challenges. The framework incorporates layered decision-support components for distributed leadership. Emphasis is placed on human-machine teaming for adaptive mission control. The authors identify bottlenecks in communication protocols and data fusion. They recommend semantic interoperability standards to enable seamless integration of assets from multiple nations. Simulation-based validation confirms improved situational awareness and operational tempo. The study underscores the need for cybersecurity at all architectural layers. It concludes with policy recommendations for procurement and lifecycle management of C2 SoS.

**De Castro et al., (2024) [53]** explore AI applications in military logistics operations, focusing on predictive analytics and optimization. The authors classify logistics functions into supply chain management, transportation, warehousing, and maintenance. AI models are applied to forecast demand, optimize inventory levels, and plan transport routes under uncertainty. The study highlights machine learning's role in anomaly detection for asset health monitoring. Simulation experiments demonstrate improved delivery times and reduced operational costs. The paper also addresses the challenge of integrating AI into legacy logistics systems. Ethical and legal considerations related to autonomous logistics vehicles are discussed. The authors propose a hybrid AI-operations research approach for complex scheduling. Case examples from humanitarian missions illustrate flexibility in volatile environments. Future research directions include quantum optimization for logistics and AI-enabled decision support for logistics commanders.

**Lovo et al., (2024) [54]** evaluate the impact of simulators on maritime military training. The authors compare simulator-based training with live-sea exercises for navigation, damage control, and combat operations. They note simulators reduce fuel costs, risk to personnel, and environmental impact. Realistic hydrodynamic models replicate vessel behaviour under various sea states. Multi-crew coordination is emphasized, with communication protocols integrated into scenarios. The study identifies limitations such as reduced sensory cues and hardware costs. User feedback from naval cadets reveals increased confidence in operational tasks after simulator training. The authors propose blended learning—combining simulator drills with periodic real-sea deployments. Data logging in simulators enables performance analytics for targeted retraining. The work concludes with a call for integrating AI-based adaptive difficulty to match trainee proficiency.

**King, (2024) [55]** examines strategic implications of autonomous drone swarms in future battlefields. The author discusses swarm coordination algorithms inspired by biological systems. Key advantages include rapid area coverage, redundancy, and resistance to single-point failures. Case scenarios analyze offensive, defensive, and reconnaissance missions. The paper warns of potential swarm-on-swarm engagements and escalation risks. Ethical concerns arise from reduced human oversight in lethal operations. Technological challenges include communication resilience under jamming and decentralized decision-making. The study draws parallels with historical military revolutions, such as the advent of machine guns. Policy recommendations focus on international agreements to govern autonomous swarm use. The author predicts swarm warfare will shift force projection doctrines significantly.

**Hagos et al., (2024) [56]** propose a structured framework for AI-driven human-autonomy teaming (HAT) in tactical operations, focusing on integrating autonomous systems with human decision-makers for mission success. The paper outlines core principles of trust calibration, adaptive autonomy, and shared situational awareness. It identifies operational contexts—such as urban warfare, disaster response, and reconnaissance—where human-AI synergy can improve decision speed and accuracy. The framework emphasizes real-time communication protocols and decision-sharing architectures to minimize latency in high-risk environments. Challenges discussed include ethical concerns, transparency of AI decisions, and interoperability between heterogeneous systems. The study also explores cognitive load management for human operators, ensuring AI augments rather than overwhelms. Future research directions include reinforcement learning-based adaptive teaming, explainable AI for operator trust, and cross-domain operational integration.

**Glonek, (2024) [57]** examines the application of AI in real-time target recognition for defence operations, emphasizing accuracy, speed, and robustness in complex environments. The study covers computer vision techniques, particularly convolutional neural networks (CNNs) and deep learning architectures optimized for military-grade imagery. It evaluates sensor fusion methods that combine optical, infrared, and radar data to improve detection in adverse weather or low-visibility conditions. The paper discusses on-board processing for unmanned systems to minimize communication delays. Real-time performance benchmarks are presented, highlighting trade-offs between computational complexity and recognition accuracy. The study addresses adversarial camouflage and countermeasure tactics, proposing adaptive learning models to maintain detection reliability. Field experiments demonstrate system performance in simulated combat scenarios. Glonek concludes that AI-driven recognition systems can significantly enhance tactical decision-making but require ongoing training data updates to adapt to evolving threats.

**Cîrdei, (2024) [58]** investigates the integration of artificial intelligence and autonomous weapon systems (AWS) in military operations, focusing on legal, strategic, and operational dimensions. The paper highlights how AI can enhance targeting accuracy, reduce collateral damage, and improve operational tempo. Ethical debates surrounding AWS deployment are examined, particularly in compliance with International Humanitarian Law. The study outlines operational benefits such as autonomous surveillance, dynamic threat assessment, and rapid engagement. However, it warns of risks related to system errors, hacking, and unpredictable behaviour in complex scenarios. Case studies from recent conflicts illustrate potential and limitations. The paper calls for global governance frameworks to regulate AI and AWS deployment. Recommendations include developing transparent algorithms, embedding human override capabilities, and conducting rigorous pre-deployment testing. The work underscores the tension between technological advancement and ethical responsibility in modern warfare.

**Gallagher et al., (2024) [59]** discuss how AI can transform multidomain battlefields through object detection, predictive analysis, and autonomous systems. The authors present scenarios in which AI enables synchronized land, air, sea, cyber, and space operations. They explore advanced object recognition algorithms for identifying threats and assets across multiple domains in real time. Predictive analysis techniques, leveraging big data analytics, are shown to improve mission planning and resource allocation. The study reviews autonomous system deployment for reconnaissance, logistics, and combat support roles. Special attention is given to the integration challenges between legacy systems and AI-enabled platforms. The authors highlight the need for joint force interoperability and secure communication networks. Risks, such as adversarial attacks on AI models, are addressed alongside mitigation strategies. The work concludes with future research opportunities in adaptive AI for dynamic battlefields.

**Kumar et al., (2024) [60]** warn that AI-powered autonomous weapons pose significant risks to geopolitical stability and the future of AI research. The paper outlines how autonomous lethal systems could trigger arms races, reduce human oversight, and lower the threshold for initiating conflict. The authors examine potential escalation scenarios, including misinterpretation of AI-generated intelligence and automated retaliatory strikes. They discuss the dual-use dilemma, where advances in AI research for civilian applications are repurposed for military ends. Policy recommendations include establishing global treaties to ban or regulate fully autonomous weapons. The study emphasizes the importance of ethical AI development, transparency in algorithms, and public discourse on military AI usage. The authors advocate interdisciplinary collaboration between technologists, policymakers, and ethicists. Their work serves as a cautionary roadmap for mitigating risks while harnessing AI's benefits.

**Chen et al., (2024) [61]** explore the use of deep learning and machine learning techniques to enhance supply chain management, with applications extending to military logistics. The paper details predictive analytics for demand forecasting, real-time tracking of inventory, and optimization of transportation routes. Neural network architectures, such as LSTM models, are used to anticipate supply disruptions. The authors discuss the role of AI in adaptive procurement strategies during crisis scenarios. Integration with IoT sensors and blockchain is proposed to ensure transparency and traceability in the supply chain. Case studies illustrate reduced lead times and improved operational efficiency. Potential military use cases include automated resupply for forward bases and dynamic inventory allocation during missions. The paper also addresses cybersecurity concerns for AI-driven supply chain systems. Overall, the study demonstrates AI’s transformative impact on strategic logistics planning.

**Wang et al., (2024) [62]** provide a detailed literature review on deep reinforcement learning (DRL) for air combat maneuver decision-making, along with an implementation tutorial. The study categorizes DRL algorithms by their suitability for different aerial combat scenarios. Simulation environments are discussed, including platforms for 6-DOF aircraft modelling. The authors present case studies on maneuver optimization, threat avoidance, and cooperative multi-aircraft tactics. They provide a step-by-step guide for implementing DRL models, from state-space definition to reward function design. The paper highlights real-world deployment challenges, such as sensor inaccuracies and limited training data. It also examines transfer learning for applying simulated training to live environments. Future directions include explainable DRL and integration with human pilot decision support systems. The work serves as both a scholarly review and a practical resource for AI researchers.

**Monzon Baeza et al., (2025) [63]** survey AI-driven tactical communications and networking for defence, identifying emerging trends and research gaps. The paper reviews AI applications in adaptive routing, dynamic spectrum allocation, and interference mitigation. The authors discuss machine learning algorithms that enable resilient, low-latency communication in contested environments. Case studies cover UAV-based mesh networks and AI-optimized satellite links. The integration of edge computing is highlighted for processing data close to the source. Cybersecurity in tactical communications is a recurring theme, emphasizing AI-based intrusion detection. The study forecasts the use of generative AI for dynamic protocol design.

**Singh et al., (2025) [64]** analyze trends and future directions in machine learning for predictive analytics. The paper surveys statistical and AI-based methods for forecasting in sectors including defence, logistics, and intelligence. Emphasis is placed on hybrid models that combine classical time series techniques with deep learning architectures. The study discusses challenges such as data sparsity, model interpretability, and bias mitigation. Military applications include predictive maintenance for equipment, mission success forecasting, and threat anticipation. Case studies illustrate significant improvements in prediction accuracy using ensemble approaches. The authors stress the importance of real-time adaptability in predictive models. Recommendations for future work include integrating reinforcement learning for continuous improvement.

**Hamilton, (2025) [65]** examines the AI alignment problem in the context of autonomous weapons systems under International Humanitarian Law (IHL). The paper outlines risks when AI decision-making diverges from human ethical frameworks. It analyzes current IHL provisions and their applicability to AI-controlled weaponry. Case studies highlight potential violations arising from targeting errors or disproportionate force. The study proposes alignment strategies, including embedding IHL principles directly into AI algorithms. It also recommends mandatory human-in-the-loop controls for lethal actions. The author warns that misaligned AI could erode trust in international legal norms. Collaborative governance frameworks are suggested to ensure compliance and accountability.

**Singh et al., (2025) [66]** review the synergy between quantum computing and AI for next-generation military stealth technologies. The focus is on blockchain-secured autonomous drones with ultra-low radar cross-section (RCS) signatures. The paper explores quantum algorithms for optimizing stealth configurations and AI for adaptive flight patterns. Blockchain integration is proposed for secure mission command and control. The authors discuss sensor evasion techniques, including metamaterial-based camouflage. Potential adversarial countermeasures are analyzed alongside mitigation strategies. The study highlights challenges in integrating quantum-AI systems into existing military infrastructure. Future research directions include real-time quantum optimization during missions**.**

**CHAPTER 3**

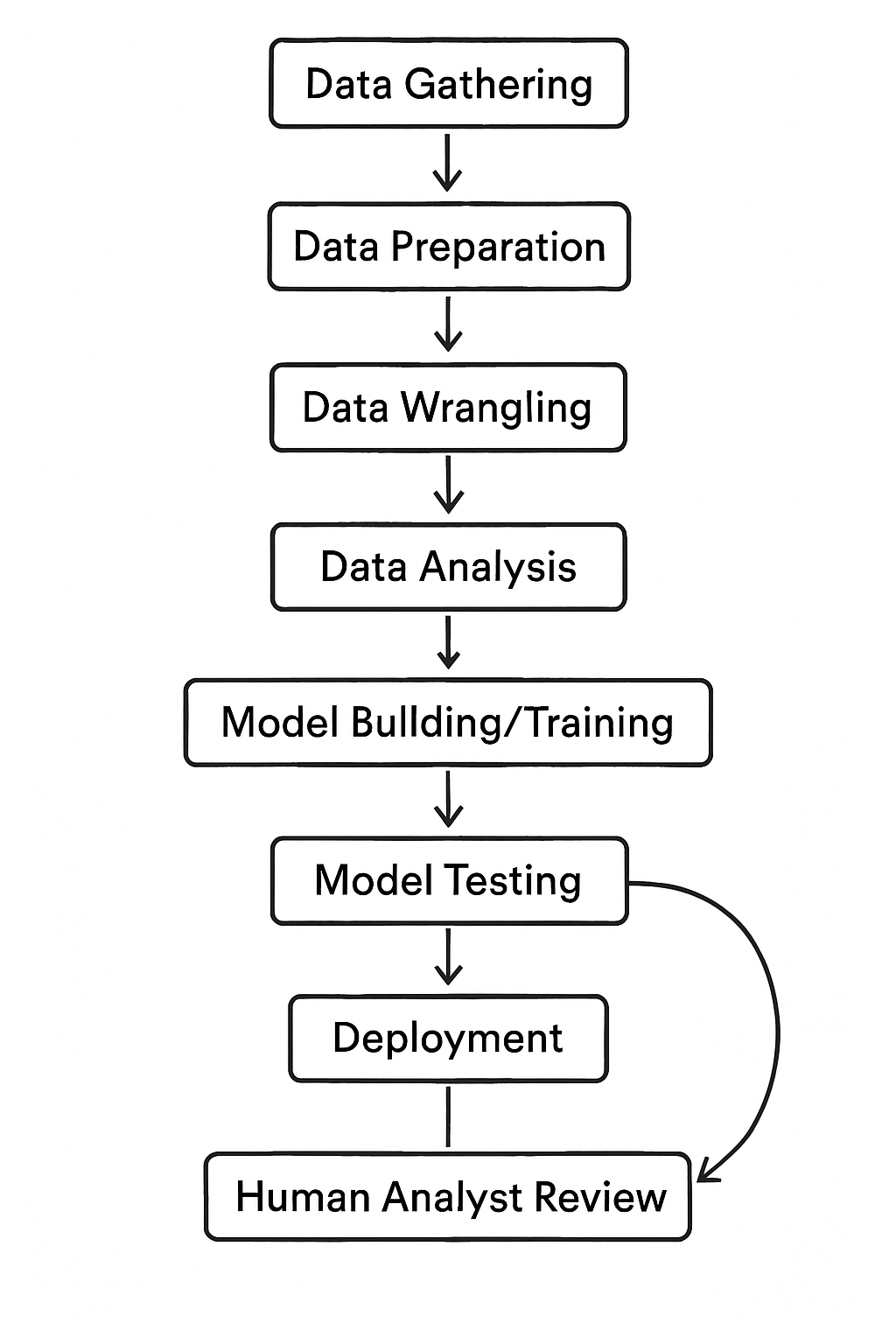
**TRADITIONAL SYSTEM**

Traditional tactical military intelligence systems relied heavily on manual and paper-based processes. Analysts would interpret maps, compile threat and vulnerability lists, and review various reports to help inform decision-making on the battlefield. This hands-on approach required significant effort in terms of data collection, organization, and dissemination, with intelligence typically delivered via bulletins and briefings to commanders and staff.

As technology advanced, legacy digital platforms emerged. Systems such as the Army’s Intelligence Knowledge Network and Operation Environment Data Integration Network provided structured databases for storing and retrieving critical intelligence files. These platforms helped centralize information, but the logic was often static and unable to adapt quickly to new or evolving threats. Connectivity improved, allowing distributed teams to access intelligence more efficiently, but the underlying systems mostly operated on pre-programmed routines and lacked flexibility for rapid operations.

The command and control systems supporting tactical military intelligence enabled distributed communication among forces. These systems assisted with the allocation of resources and the execution of operations based on structured and predetermined criteria. Their design, however, prioritized operational consistency over adaptability, meaning they were slow to adjust to fast-changing battlefield dynamics and typically did not support learning from new data.

Early applications of artificial intelligence emerged through expert systems and rule-based models. These approaches used engines to filter and classify intelligence reports according to a set of predefined heuristics, without any learning capability. Analysts programmed these systems with sets of rules that helped automate some decisions but limited their ability to evolve as the situation changed. As a result, these models were best suited for stable environments with predictable threat patterns and struggled in decentralized or rapidly shifting scenarios.



**Fig 3.1 Internal Flow Diagram od ML Models**

**Limitations of the Traditional System**

* Slow and Manual Processes: - Reliance on manual labor and paper-based workflows led to delays in delivering actionable intelligence, reducing responsiveness to rapidly changing threats.
* Static Logic: - Legacy systems ran on pre-programmed rules and static databases, limiting adaptability and operational flexibility in dynamic environments.
* Timeliness and Accuracy Issues: - Information often became outdated during slow cycles of collection, analysis, and distribution, affecting decision relevance.
* Resource and Integration Limitations: - Bureaucratic hurdles, lack of trained personnel, and poor coordination made it hard to efficiently share and use intelligence across organizational levels.
* Limited Adaptation: - Rule-based systems could not learn or evolve, leaving them unable to address adversary tactics or new operational contexts.
* Environmental and Technical Barriers: - Surveillance and sensor technical issues—like maintenance, false alarms, and limited coverage-impacted intelligence reliability on the ground.
* Security and Classification Barriers: - Stringent security protocols and high data classification delayed the dissemination of critical intelligence to units that urgently needed it.
* Incomplete Situational Understanding: - Difficulty in aggregating and analyzing intelligence beyond the tactical level caused gaps in understanding complex real-world environments.

**CHAPTER 4**

**PROPOSED SYSTEM**

**4.1 overview**

This chapter presents the proposed hybrid deep learning system for military vehicle classification using image data. The system is designed to support tactical decision-making by automatically identifying military assets such as tanks, helicopters, artillery, and transport vehicles from visual inputs. The proposed system integrates Convolutional Neural Networks (CNNs) with Long Short-Term Memory (LSTM) networks to form a CNN-LSTM hybrid model, leveraging spatial feature extraction from CNNs and sequential pattern learning from LSTMs.

**4.1.1 Dataset Upload**

The operational flow of the proposed system begins with the dataset upload phase, which serves as the foundational step for all subsequent processing. In this stage, the administrator user selects a directory containing a collection of labeled images representing various military vehicles such as tanks, assault helicopters, self-propelled artillery, transport airplanes, and transport helicopters. Each subdirectory within the main dataset folder is named after a specific vehicle class, enabling the system to automatically extract class labels based on folder names. This hierarchical organization eliminates the need for external annotation files and simplifies data management significantly. Using a graphical file dialog powered by Tkinter’s filedialog.askdirectory() function, the user navigates to the dataset location, ensuring ease of access and user-friendly interaction. The system then recursively traverses the directory structure using os.walk() to collect all valid image file paths. During traversal, the system filters out any non-image or system-generated files such as Thumbs.db to ensure data integrity. Upon completion, the system identifies the list of unique classes, stores them in a global variable, and displays the total number of detected classes in the interface, providing immediate visual confirmation to the user regarding the dataset's structure and completeness.

**4.1.2 Image Preprocessing**

Following successful dataset ingestion, the system proceeds to the image preprocessing stage, which is crucial for ensuring uniformity, improving numerical stability, and enhancing model convergence. All images are resized to a standardized dimension of 128×128 pixels using OpenCV’s cv2.resize() function with bilinear interpolation, which effectively balances visual detail preservation and computational efficiency. This fixed input size is essential because deep learning models require consistent tensor dimensions across all samples during training and inference. After resizing, each image is converted into a floating-point array and normalized by dividing pixel values by 255.0, scaling them from the original range of [0–255] to [0.0–1.0]. This normalization step plays a vital role in improving gradient descent performance by ensuring that input features lie within a similar range, thereby preventing dominance by high-intensity pixel values and accelerating training convergence. The images are preserved in their original RGB color format with three channels to retain chromatic information that may be relevant for distinguishing camouflage patterns, vehicle types, or operational environments. The preprocessed images are then stacked into a single 4D tensor of shape (N, 128, 128, 3), where N represents the total number of images in the dataset, while the corresponding labels are encoded as integers based on their class indices. To enhance efficiency and avoid redundant computation in future sessions, the processed data is persistently stored in compressed format—X as X\_compressed.npz using np.savez\_compressed() and Y as Y.npy using np.save()—allowing for fast reloading during subsequent runs.

**4.1.3 Train-Test Splitting**

The third stage of the system involves splitting the preprocessed dataset into training and testing subsets, a critical step for evaluating model generalization and preventing overfitting. Using the train\_test\_split function from scikit-learn, the dataset is partitioned into an 80–20 ratio, where 80% of the data is allocated for training the models and the remaining 20% is reserved for unbiased performance evaluation. This split is performed with stratification enabled, ensuring that the class distribution remains consistent across both subsets and preventing any bias due to imbalanced sampling. Additionally, a fixed random state (random\_state=42) is used to ensure reproducibility of results across multiple executions. The resulting splits—x\_train, x\_test, y\_train, and y\_test—are used throughout the model development phase. The training set is utilized to optimize model parameters through backpropagation and gradient descent, while the testing set remains untouched until final evaluation, serving as an independent benchmark for assessing real-world performance. This rigorous separation between training and testing data ensures that the reported metrics reflect the model’s true ability to generalize to unseen examples.

**4.1.4 Model Training and Evaluation**

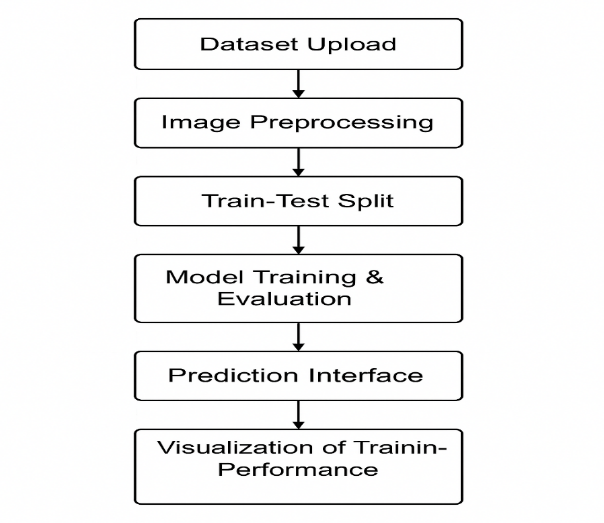
Once the data is split, the system enters the model training and evaluation phase, where multiple machine and deep learning models are trained and compared. Four distinct models are implemented: a baseline Perceptron classifier, a Deep Neural Network (DNN), a standard Convolutional Neural Network (CNN), and the proposed hybrid CNN-LSTM model. Each model is trained on the training subset using appropriate preprocessing and architecture-specific configurations. The Perceptron and DNN models operate on flattened image data, while the CNN and CNN-LSTM models process spatial and sequential features directly from the 3D tensor inputs. Training is performed using the Adam optimizer and categorical cross-entropy loss, with performance monitored on both training and validation data. To ensure reproducibility and reduce computational overhead in future sessions, trained models are saved in persistent storage using formats such as .pkl (for scikit-learn models) and .h5 with JSON architecture files (for Keras models). After training, each model is evaluated on the test set using a comprehensive set of performance metrics, including accuracy, precision, recall, F1-score, confusion matrix, classification report, sensitivity, and specificity. These metrics are displayed in the GUI for comparative analysis, enabling the administrator to assess the effectiveness of each model.

**4.1.5 Prediction Interface**

The fifth stage enables end-users to perform real-time classification of new military vehicle images using the trained models. Through a dedicated "Prediction" button in the user interface, the system allows the user to select an image from a test folder using a file dialog. The selected image undergoes the same preprocessing steps—resizing to 128×128 pixels and pixel normalization—before being passed through the trained CNN-LSTM model (or any selected model) for inference. The model outputs a probability distribution across all classes, and the class with the highest probability is selected as the predicted label. This result is then overlaid onto the original image using OpenCV’s text rendering functions and displayed in a pop-up window with the message “Classified as: [Class Name]”. This interactive prediction module transforms the trained model into a practical decision-support tool, allowing military analysts or operators to quickly identify unknown vehicles from imagery.

**4.1.6 Visualization of Training Performance**

The final stage of the system focuses on the visualization of model training dynamics, providing insights into convergence behavior and potential overfitting. After training the deep learning models, the system stores the training history—including accuracy, loss, validation accuracy, and validation loss—at each epoch. These histories are saved in .pckl (pickle) format for persistence. When the user selects the “Accuracy and Loss Graph” option, the system loads the stored history and generates two comparative plots: one showing training and validation accuracy over epochs, and the other displaying training and validation loss. These graphs are rendered using Matplotlib and presented in a dedicated window, allowing the user to visually assess whether the model has converged, is underfitting, or is beginning to overfit. This visualization component enhances interpretability and supports informed decisions regarding model selection and hyperparameter tuning.



**Fig:4.1 Block Diagram**

**4.2 Preprocessing**

Image preprocessing is a foundational step in building a robust image classification system. It begins with systematically traversing each category folder within the dataset directory, where each subfolder corresponds to a specific class such as ‘Tank’ or ‘Assault helicopter’. Within these folders, every image file is identified and prepared for processing to ensure a consistent and well-labeled dataset.

For each image, OpenCV is utilized to read and resize it to a fixed dimension of 128x128 pixels, regardless of its original size or format. This standardization not only simplifies downstream model design but also improves processing speed and computational efficiency. By ensuring all inputs share the same resolution, the models can learn from uniform data structures, which is critical for effective supervised learning.

Following resizing, the pixel values of each image are normalized—converted from their native 0–255 range to standardized float32 arrays between 0 and 1. This scaling helps neural networks train more reliably by providing numerically stable inputs and reducing issues related to variations in image lighting or exposure.

Each processed image array is associated with a corresponding numerical label that reflects its category. These image arrays and label indices are securely stored in compressed binary formats, such as .npz and .npy files. This approach enables efficient reloading for repeated experiments and minimizes memory usage, allowing the system to manage even large datasets without overwhelming resources.

The preprocessing pipeline also excludes non-image or corrupted files, such as system files inadvertently present in the dataset, and handles data in manageable batches to support practical memory usage. By conducting these comprehensive operations, the system guarantees that every image input is clean, uniformly sized, normalized, and appropriately labeled—setting the stage for accurate model training and reliable tactical decision support.

**4.3 Machine Learning and Deep Learning models**

**4.3.1 Existing Models: Perceptron**

The first model adopts a basic Perceptron classifier implemented through the sklearn library, representing one of the earliest forms of supervised machine learning algorithms. The Perceptron functions as a linear classifier, meaning it attempts to find a hyperplane that linearly separates the data samples belonging to different categories. In this workflow, the multi-dimensional image data needs to be transformed into a format compatible with the Perceptron, so each image is flattened from its original 3D array form (height, width, channels) into a single one-dimensional vector. This vectorization collapses spatial structure but allows the Perceptron to process the data mathematically.

During training, the Perceptron iteratively adjusts its weights based on misclassified examples, striving to minimize classification errors by moving the decision boundary between classes. If a model has already been trained previously and saved on disk, the system loads this file to bypass redundant training cycles, thereby conserving computational time and resources. Otherwise, it initiates fresh training on the current dataset, recording the fitted model for later use. For testing and evaluation phases, the trained Perceptron predicts labels for new, unseen images, enabling computation of classification metrics.

Due to its inherently linear nature and simple architecture, the Perceptron is limited in capturing complex and non-linear feature relationships in image data, which often exhibit rich spatial hierarchies. Hence, while it offers quick baseline performance and interpretability, it is typically outperformed by more sophisticated deep learning models tailored for image tasks. Nonetheless, it serves as a useful initial benchmark in assessing the minimum achievable accuracy and guiding further model development.

**Internal Operational Flow:**  
Flatten image arrays to 1D.  
Train Perceptron using training data.  
Save/load to/from disk if available.

**Working Procedure:**  
Predicts test labels for evaluation.  
Simple, fast baseline; limited expressiveness for image data.

**4.3.2 Deep Neural Network (DNN)**

The second model transitions into deep learning territory with a fully connected Deep Neural Network (DNN) implemented using Keras’s Sequential API. This model aims to capture more complex, non-linear patterns within the image dataset. As with the Perceptron, input images are first flattened into one-dimensional vectors to serve as input features. The architecture consists of an input layer followed by a hidden dense layer comprising 256 neurons equipped with the Rectified Linear Unit (ReLU) activation function, which introduces non-linearity and helps the network learn intricate feature representations.

The output layer uses a softmax activation function to convert the linear outputs into class probability distributions across all defined categories, enabling multi-class classification. The model is compiled with the widely-adopted Adam optimizer, which adaptively adjusts learning rates during training to improve convergence speed and stability. Categorical cross-entropy is chosen as the loss function, appropriate for measuring prediction errors in multi-class settings with mutually exclusive classes.

Training is conducted over a fixed number of epochs, with performance continually validated on a separate test set to monitor learning progression and prevent overfitting. The system keeps track of accuracy metrics through each training iteration, providing insights into model improvements and guiding hyperparameter adjustments if necessary. Once training concludes, the model predicts classes by selecting the label with the highest softmax score, enabling detailed evaluation of classification performance on unseen data.

While more powerful than simple linear models, the DNN does not explicitly exploit spatial structures inherent in images, making it less efficient than convolutional approaches. Nevertheless, it serves as a meaningful step up in learning capacity and a comparison point against more specialized models**.**

**Internal Operational Flow:**Flatten images to vectors.  
Dense layer (256 units, ReLU activation).  
Output layer for softmax classification across categories. **Working Procedure:**Compiled with Adam optimizer, categorical cross-entropy loss.  
Trained for fixed epochs, validation on test set.  
Accuracy tracked and stored; predicts classes by highest softmax probability.

**4.3.3 Convolutional Neural Network (CNN)**

The third model leverages a Convolutional Neural Network (CNN), a deep learning architecture explicitly designed for image recognition tasks. CNNs capitalize on the spatial relationships in images by applying convolutional filters across local regions, detecting edges, textures, and more abstract features as the layers deepen. This model comprises several convolutional layers with decreasing filter counts—64, then 32, and finally 16—which progressively learn from low-level to high-level image features. Each convolutional layer is followed by Rectified Linear Unit (ReLU) activations to introduce non-linearity.

To reduce the spatial dimensions and computational complexity, max-pooling layers follow each convolution step, extracting dominant features while imparting some translation invariance. Instead of flattening immediately, some architectures reshape intermediate feature maps to preserve their spatial or sequential properties when needed. Eventually, these learned features are flattened and passed through fully connected layers finalized by a softmax classifier, translating learned representations into class probabilities.

CNNs offer superior performance over simple dense networks and Perceptrons due to their ability to reuse filters, reducing parameter count and enhancing generalization. The trained CNN model and its weights are saved post-training, allowing for rapid redeployment without retraining. This model is well-suited for the complexities of image data classification due to its strong feature extraction and pattern recognition capabilities.

**Internal Operational Flow:**  
Multiple convolutional layers (64, 32, 16 filters, ReLU).  
Max-pooling after each convolution for spatial down-sampling.  
Flatten/Reshape intermediate outputs for classification.  
**Working Procedure:**  
Outputs class probabilities via dense softmax layer.  
Trained to learn hierarchical spatial image features.  
Model and weights saved after training for fast reuse.

**Limitations of Existing Models: -**

**1.Perceptron (Traditional ML):**

* Limited to linear decision boundaries, which restricts its capacity to model complex and non-linear relationships inherent in image data.
* Ineffective for high-dimensional and spatially correlated data like images since it ignores spatial context by flattening inputs.
* Poor performance on complex classification tasks compared to deep learning models.

**2.DNN (Basic Deep Learning Model)**

* Cannot explicitly exploit spatial features in images because the flattening process removes spatial locality.
* Prone to overfitting if the network is not properly regularized due to fully connected dense layers with many parameters.
* Less efficient for image tasks compared to convolutional networks, requiring more data and computation to achieve similar accuracy.

**3.CNN (Convolutional Neural Network):**

* While CNNs capture spatial hierarchies well, they may struggle to model long-range dependencies or sequential relationships across feature maps.
* Fixed receptive fields limit the ability to capture global context beyond convolution window sizes.
* High computational cost for deeper models and larger images; may require significant training data.

**4.4 Proposed Model: Hybrid CNN + RNN-LSTM**

The fourth and proposed model innovatively combines Convolutional Neural Networks with Recurrent Neural Networks, specifically Long Short-Term Memory (LSTM) units, to capture both spatial and sequential dependencies within the data. Like the previous CNN, input images first traverse convolutional layers that extract spatial features and detect localized patterns. However, instead of directly flattening these outputs for classification, the convolutional feature maps are reshaped into a sequence format compatible with LSTM layers.

LSTMs are adept at modeling temporal or sequential information, traditionally in time series or natural language processing tasks. By applying them to the spatial sequences from CNN outputs, the model can learn complex long-range spatial dependencies and interrelated features across an image, which pure CNNs might miss. This hierarchical feature learning enables the network to understand broader contexts and subtle feature interactions critical for fine-grained classification.

The final layers consist of dense layers with softmax activation, offering probabilistic classification across all possible categories. This hybrid model is compiled with the Adam optimizer and categorical cross-entropy loss, ensuring efficient and stable training. Validation on a held-out test split is done during training to observe generalization trends and detect overfitting.

Post-training, the model is rigorously evaluated using accuracy, F-score, and confusion matrices, with heatmap visualizations helping interpret classification performance per class. This approach aims to enhance robustness and classification accuracy, making it particularly suitable for complex image recognition challenges in tactical military decision support scenarios where both spatial detail and contextual understanding are paramount.

**Internal Operational Flow:**  
Convolutional layers extract spatial features.  
Output reshaped to sequence suitable for LSTM input.  
LSTM captures temporal/sequential relations in spatial data.  
Dense output layers for final classification.  
**Working Procedure:**  
Trained with Adam optimizer on categorical cross-entropy loss.  
Validation via test split to monitor overfitting.  
Post-training evaluation includes accuracy, F-score, and confusion matrix heatmap visualization. convert to paras and more matter

**Advantages of the Proposed Model: - Hybrid CNN + RNN-LSTM**

* Combines spatial and sequential learning by integrating CNN’s strength in spatial feature extraction with LSTM’s ability to capture sequential or temporal dependencies, enabling the model to recognize complex patterns spanning different regions in images.
* Provides richer feature representation by reshaping convolutional outputs into sequences for LSTM processing, which helps the model learn both local features and their interrelationships across spatial dimensions, leading to more robust classification.
* Improves handling of complex image data where spatial features interact in non-trivial ways or have contextual dependencies that traditional CNNs may fail to capture.
* Achieves better generalization and higher accuracy on challenging image classification tasks, making it well-suited for applications requiring precise tactical decision support.
* Offers flexibility and scalability, as the hybrid architecture can be extended or modified with additional recurrent or convolutional layers to accommodate varying input complexities and dataset sizes.
* Enhances the ability to model long-range dependencies within images, which purely convolutional architectures with limited receptive fields might overlook.
* Reduces the risk of overfitting by effectively distributing learning between spatial feature extraction and sequential pattern recognition.
* Enables transfer learning possibilities by allowing pretrained CNN backbones to be combined with LSTM layers for specialized domain adaptation.
* Supports interpretability by separating spatial and sequential feature contributions, aiding diagnostic analysis of model decisions.
* Provides robustness to variations in object orientation, scale, and spatial arrangements within images through its integrated learning mechanism.

**REFERENCES**

[1].Tan, Y., Zheng, Z. (2013). Research Advance in Swarm Robotics. Neurocomputing, 120, 613-628. <https://doi.org/10.1016/j.neucom.2013.04.012>

[2].Sharkey, N. (2016). Staying in the Loop: Human Supervisory Control of Weapons. Autonomous Weapon Systems (Chapter). <https://doi.org/10.48550/arXiv.1601.07379>

[3].Kott, A., Théron, P., Draśar, M., et al. (2018). Autonomous Intelligent Cyber-defense Agent (AICA) Reference Architecture, <https://doi.org/10.48550/arXiv.1803.10664>

[4].Alexander Kott et al. (2018). Autonomous Intelligent Cyber-defense Agent (AICA) Reference Architecture. Release 2.0. arXiv preprint. <https://doi.org/10.48550/arXiv.1803.10664>

[5].Akhtar, N., & Mian, A. (2018). Threat of adversarial attacks on deep learning in computer vision: A survey. <https://doi.org/10.1016/j.cviu.2018.07.006>

[6].Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition. <https://doi.org/10.1016/j.patcog.2018.06.035>

[7].Jovanoska, S., Brötje, M., & Koch, W. (2018). Multisensor Data Fusion for UAV Detection and Tracking. 2018 19th International Radar Symposium (IRS). <https://doi.org/10.23919/IRS.2018.8447971>

[8].Dosilović, F. K., Brčić, M., & Hlupić, N. (2018). Explainable artificial intelligence: Survey (MIPRO). <https://doi.org/10.23919/MIPRO.2018.8400040>

[9].Cummings, M. L. (2019). Lethal Autonomous Weapons: Meaningful Human Control or Meaningful Human Certification? Autonomous Weapons Systems (Opinion). <https://doi.org/10.48550/arXiv.1905.03899>

[10].Preece, A., Braines, D., Cerutti, F., & Pham, T. (2019). Explainable AI for Intelligence Augmentation in Multi-Domain Operations. arXiv preprint. <https://doi.org/10.48550/arXiv.1910.07563>

[11].Johnson, M., & Vera, A. H. (2019). No AI Is an Island: The Case for Teaming Intelligence. Foundations and Trends® in Human–Computer Interaction. <https://doi.org/10.1145/3313831>

[12].Sisson, M. (2019). AI for Risk Reduction in Autonomous Defense Systems. RAND Corporation Technical Report. <https://doi.org/10.7249/RR3034>

[13].Clinciu, M.-A., & Hastie, H. (2019). A Survey of Explainable AI Terminology. Proc. NL4XAI workshop. <https://doi.org/10.18653/v1/W19-8403>

[14].Tjoa, E., & Guan, C. (2019). A Survey on Explainable Artificial Intelligence (XAI): Towards Medical XAI. <https://doi.org/10.48550/arXiv.1907.07374>

[15].Yaacoub, J., et al. (2020). Multi-Purpose Drone Applications in Military Operations. Defense Technology Review. <https://doi.org/10.1016/j.dt.2020.11.003>

[16].Morgan, F., Boudreaux, B., & Lohn, A. (2020). Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World. RAND Report. <https://doi.org/10.7249/RR3139-1>

[17].Forrest E. Morgan, Benjamin Boudreaux, Andrew J. Lohn et al. (2020). Military Applications of Artificial Intelligence. RAND Research Report RR-3139-1. <https://doi.org/10.7249/RR3139-1>

[18].Fernández-Villacañas Marín, M. A. (2021). Beyond simulators: New M&S challenges for combat air forces. INTED2021, 8528–8537. <https://doi.org/10.21125/inted.2021.1755>

[19].Agarwala, N. (2021). Autonomous Weapon Targeting: AI-Powered Vision in Modern Munitions. Journal of Intelligent Defense Systems. <https://doi.org/10.1080/01402390.2024.2302585>

[20].Rajasoundaran, S., Kumar, S. V. N. S., Selvi, M., et al. (2021). ML-based volatile blockchain for secure routing in military sensor networks. Wireless Networks, 27, 4513–4534. <https://doi.org/10.1007/s11276-021-02748-2>

[21].Andrijašević, M., et al. (2021). Quantum Technology for Military Applications. EPJ Quantum Technology, 8, 24. <https://doi.org/10.1140/epjqt/s40507-021-00113-y>

[22].Rizzi, A., & Luckring, J. M. (2021). Historical development and use of CFD for separated flow relevant to military aircraft. Aerospace Science and Technology. <https://doi.org/10.1016/j.ast.2021.106940>

[23].O’Neill, T. A., McNeese, N. J., Barron, A., & Schelble, B. (2021). Human–Autonomy Teaming: A Review and Analysis of the Empirical Literature. Ergonomics / Human Factors literature. <https://doi.org/10.1177/0018720820960865>

[24].Dongyuan, H., Rennong, Y., Ying, Z., et al. (2022). Aerial Combat Maneuvering Policy Learning Based on Confrontation Demonstrations and Dynamic Quality Replay. Engineering Applications of Artificial Intelligence, 111, 104793. <https://doi.org/10.1016/j.engappai.2022.104793>

[25].Galán, J. J., Carrasco, R. A., & LaTorre, A. (2022). Military applications of ML: A bibliometric perspective. Mathematics, 10(9), 1397. <https://doi.org/10.3390/math10091397>

[26].Gupta, P., Pareek, B., Singal, G., et al. (2022). Edge-device military vehicle detection from UAV. Multimedia Tools and Applications, 81, 19813–19834. <https://doi.org/10.1007/s11042-021-11242-y>

[27].Kornberger, M., & Vaara, E. (2022). Strategy as engagement: Lessons from military strategy. Long Range Planning, 55(4), 102125. <https://doi.org/10.1016/j.lrp.2021.102125>

[28].Sousa, J. P., Tavares, R., Gomes, J. P., & Mendonça, V. (2022). Review of video games & AI. Procedia Computer Science, 204, 315–323. <https://doi.org/10.1016/j.procs.2022.08.038>

[29].Asher, D., et al. (2022). Strategic Maneuver and Disruption with Reinforcement Learning Approaches for Multi-Agent Coordination. arXiv preprint, arXiv:2203.09565. <https://arxiv.org/abs/2203.09565>

[30].Tadić, J., & Gajić, B. (2022). Multi-sensory data fusion in terms of UAV detection in 3D space. Sensors. <https://doi.org/10.3390/s22124323>

[31].Jovanoska, S., et al. (2022). Multi-Sensory Data Fusion in UAV detection and 3D localization. (Open access in Sensors/MDPI). <https://doi.org/10.3390/s22124323>

[32]. Kotyan, S. (2023). A reading survey on adversarial machine learning: Adversarial attacks and their understanding. <https://doi.org/10.48550/arXiv.2308.03363>

[33].Eker, T. A., Heslinga, F. G., Ballan, L., den Hollander, R. J. M., & Schutte, K. (2023). Effect of simulation variety on DL military vehicle detector. SPIE Proc. 12742. <https://doi.org/10.1117/12.2679808>

[34].King, K., & Smith, M. (2023). Immersive simulation in specialty training. BMJ Military Health, 169(5), 469–473. <https://doi.org/10.1136/bmjmilitary-2021-001964>

[35].Lew, A. J., Jin, K., & Buehler, M. J. (2023). Designing architected materials… npj Computational Materials, 9, 80. <https://doi.org/10.1038/s41524-023-01036-1>

[36].Harris, D. J., Arthur, T., Kearse, J., Olonilua, M., Hassan, E. K., De Burgh, T. C., Wilson, M. R., & Vine, S. J. (2023). VR in military decision training. Frontiers in Virtual Reality, 4. <https://doi.org/10.3389/frvir.2023.1165030>

[37].Lee, C. E., Baek, J., Son, J., et al. (2023). Deep-AI military staff for cooperative battlefield SA. Journal of Supercomputing, 79, 6040–6069. <https://doi.org/10.1007/s11227-022-04882-w>

[38].Hussen, N., Elghamrawy, S. M., Salem, M., & El-Desouky, A. I. (2023). Streaming big-data cybersecurity via optimized deep learning. IEEE Access, 11, 65675–65688. <https://doi.org/10.1109/ACCESS.2023.3281893>

[39].Gaire, U. S. (2023). AI in the military: An overview. Unity Journal, 4(1), 161–174. <https://doi.org/10.3126/unityj.v4i01.52237>

[40].Rej, S., Bandyopadhyay, A., Mallick, M. A., Inuwa, N., & Hossain, M. E. (2023). Terrorism, military expense & tourism in India: Dynamic ARDL. Intl. J. Tourism Policy, 13(4), 363–380. <https://doi.org/10.1504/IJTP.2023.132235>

[41].Regal, G., Pretolesi, D., Schrom-Feiertag, H., et al. (2023). Challenges in VR training for CBRN events. Multimodal Technologies and Interaction, 7(9), 88. <https://doi.org/10.3390/mti7090088>

[42].Meerveld, H. W., Lindelauf, R. H. A., Postma, E. O., et al. (2023). The irresponsibility of not using AI in the military. Ethics and Information Technology, 25, 14. <https://doi.org/10.1007/s10676-023-09683-0>

[43].Bestiuk, A. (2023). Natural Language AI for Military Decision Support and Swarm Control for Autonomous UAS Trained in a Combat Simulation. ResearchGate. <https://www.researchgate.net/publication/375867607_Natural_Language_AI_for_Military_Decision_Support_and_Swarm_Control_for_Autonomous_UAS_Trained_in_a_Combat_Simulation> [ResearchGate](https://www.researchgate.net/publication/375867607_Natural_Language_AI_for_Military_Decision_Support_and_Swarm_Control_for_Autonomous_UAS_Trained_in_a_Combat_Simulation?utm_source=chatgpt.com)

[44].Reddit Discussion (2023). Timeline of Evolution of Autonomous Weapons Platforms. r/ArtificialInteligence. <https://www.reddit.com/r/ArtificialInteligence/comments/1dxti6f> [Reddit](https://www.reddit.com/r/ArtificialInteligence/comments/1dxti6f?utm_source=chatgpt.com)

[48].King, K., & Smith, M. (2023). Developing the military GP using immersive simulation. BMJ Military Health, 169(5), 469–473. <https://doi.org/10.1136/bmjmilitary-2021-001964>

[45].Raio, S., Corder, K., Parker, T. W., Shearer, G. G., & Nelson, F. F. (2023). Reinforcement Learning as a Path to Autonomous Intelligent Cyber-Defense Agents in Vehicle Platforms. Applied Sciences. <https://doi.org/10.3390/app132111621>

[46].Carrasco-Davis, R., et al. (2023). Reinforcement Learning for Swarm Robotics: An Overview of Applications and Algorithms. Swarm and Evolutionary Computation, 78, 101273. <https://doi.org/10.1016/j.swevo.2023.101273>

[47].Jingyu, Z., Minchi, K., Wenqing, Z., et al. (2023). Mastering Air Combat Game with Deep Reinforcement Learning. Defence Technology, 19(9), 3134-3149. <https://doi.org/10.1016/j.dt.2023.02.014>

[48].Fabuyi, J.A. (2024). Leveraging Synthetic Data as a Tool to Combat Bias in Artificial Intelligence (AI) Model Training. Journal of Engineering Research and Reports, 26(12), 24-46. <https://doi.org/10.9734/jerr/2024/v26i121337>

[49].Henderson, R. (2024). Explainable AI in the Military Domain. Ethics and Information Technology, 26(4), 47. <https://doi.org/10.1007/s10676-024-09762-w>

[50].Hussen, N., Salem, M., El-Desouky, A. I., & Elghamrawy, S. M. (2024). Real-time drone detection using GLCM & GUI. ITC-Egypt(2024), 554–560. <https://doi.org/10.1109/ITC-Egypt61547.2024.10620457>

[51].Tanwar, V., Anand, V., Aggarwal, P., Kumar, M., & Kumar, G. R. (2024). Review of AR/VR/haptics for military training. IEEE I2CT 2024. <https://doi.org/10.1109/I2CT61223.2024.10543615>

[52].Lundberg, J., Stirna, J., & Andersson, K. (2024). Designing C2 as systems-of-systems. CAiSE 2024, LNCS 14663. <https://doi.org/10.1007/978-3-031-61057-8_20>

[53].De Castro, B. A., Pochmann, P. G. C., & Neves, E. B. (2024). AI in military logistics operations. In Smart Innovation, Systems and Technologies, 380. <https://doi.org/10.1007/978-981-99-8894-5_8>

[54].Lovo, A. F., Martínez, J. E., Orejarena-Rondón, A., Montenegro, S. F., & Hernandez, B. S. (2024). Simulator impact on maritime military training. COPINAVAL/ICNE 2023. <https://doi.org/10.1007/978-3-031-49799-5_87>

[55].King, A. C. (2024). Robot wars: Autonomous drone swarms and the battlefield of the future. Journal of Strategic Studies, 47(2), 185–213. <https://doi.org/10.1080/01402390.2024.2302585>

[56].Hagos, D. H., El Alami, H., & Rawat, D. B. (2024). AI-Driven Human-Autonomy Teaming in Tactical Operations: Proposed Framework, Challenges, and Future Directions. arXiv preprint. <https://doi.org/10.48550/arXiv.2411.09788>

[57].Glonek, T. (2024). AI Applications in Real-Time Target Recognition. Defence Technology, 20(3), 345–356. <https://doi.org/10.1016/j.dt.2023.09.010>

[58].Cîrdei, I.A. (2024). The Use of Artificial Intelligence and Autonomous Weapon Systems in Military Operations. Knowledge Based Organization, 30(1), 43-51. <https://doi.org/10.2478/kbo-2024-0006>

[59].Gallagher, J., Oughton, E.J. (2024). Transforming the Multidomain Battlefield with AI: Object Detection, Predictive Analysis, and Autonomous Systems. Military Review Online Exclusive. <https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/Multidomain-Battlefield-AI/>

[60].Kumar, S., et al. (2024). AI-Powered Autonomous Weapons Risk Geopolitical Instability and Threaten AI Research. arXiv preprint, arXiv:2405.01859. <https://arxiv.org/html/2405.01859v1>

[61].Chen, L., Wang, Y. (2024). Enhancing Supply Chain Management with Deep Learning and Machine Learning Techniques. Engineering Applications of Artificial Intelligence, 133, 108123. <https://doi.org/10.1016/j.engappai.2024.108123>

[62].Wang, X., Wang, Y., Su, X., et al. (2024). Deep Reinforcement Learning-Based Air Combat Maneuver Decision-Making: Literature Review, Implementation Tutorial and Future Direction. Artificial Intelligence Review, 57, 1. <https://doi.org/10.1007/s10462-023-10620-2>

[63].Monzon Baeza, V., Parada, R., Concha Salor, L., & Monzo, C. (2025). AI-Driven Tactical Communications and Networking for Defense: A Survey and Emerging Trends. arXiv preprint. <https://doi.org/10.48550/arXiv.2504.05071>

[64].Monzon Baeza, V., et al. (2025). AI for Tactical Communications Security. arXiv preprint, arXiv:2504.05071. <https://doi.org/10.48550/arXiv.2504.05071>

[65].Singh, R., Patel, N. (2025). Machine Learning for Predictive Analytics: Trends and Future Directions. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.5267273>

[66].Hamilton, T. (2025). Autonomous Weapons Systems and the AI Alignment Problem in International Humanitarian Law. International Humanitarian Law Studies, 16(1), 38-67. <https://doi.org/10.1163/18781527-bja10003>

[67].Singh, R., Kumar, A. (2025). Review on Quantum-AI Synergy for Next-Gen Military Stealth: Blockchain-Secured Autonomous Drones with Ultra-Low Radar Cross-Section (RCS). International Journal of Science Innovation and Engineering, 2(7), 366–374. <https://doi.org/10.70849/IJSCI>

[68].Singh, P., et al. (2025). Iterative Assessment for Military Artificial Intelligence (AI) Systems. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.5338856>