Journal of the Serbian Society for Computational Mechanics / Vol. 19 / No. 2, 2025 / pp 19-31 / original paper
(10.24874/jsscm.2025.19.02.02)

REXCOM (REXHEP COMMAND OPERATIONS MODULE): A HUMAN-CENTRIC MILITARY AI CHATBOT FRAMEWORK FOR SECURE COMMAND, PERSONNEL AND LOGISTICS OPERATIONS

Rexhep Mustafovski[1] [0009-0000-3257-0989], Aleksandar Petrovski[2] [0000-0002-5265-5813] and Marko Radovanović[3*] [0000-0002-9866-9639]

[1] University Goce Delcev' – Stip, Military Academy "General Mihailo Apostolski", Skopje – 1000, Republic of North Macedonia
[2] 'University Goce Delcev' – Stip, Military Academy "General Mihailo Apostolski", Skopje – 1000, Republic of North Macedonia
[3] Military Academy, University of Defence, 11000, Belgrade, Serbia
**corresponding author*

Abstract

The rapid development of artificial intelligence in military contexts has created a need for adaptive, secure, and mission-focused systems that respond to dynamic command requirements and classified environments. This paper introduces REXCOM, a novel AI chatbot framework designed specifically for military use, integrating classified command generation, personnel management, and logistics databases into a single intelligent interface. REXCOM functions on hierarchical access control, enabling users to access and generate data only up to their authorized classification level. The system also automates repetitive command drafting and supports decision-making in real time. Unlike existing military AI assistants, REXCOM integrates personnel and logistics operations with secure communication workflows, resulting in improved operational speed, accuracy, and human-AI collaboration. We evaluate REXCOM against existing systems in terms of security compliance, contextual awareness, and system integration, providing comparative graphs and performance insights.

Keywords: military chatbot, command automation, AI logistics assistant, secure access control, REXCOM, classified command system.

1. Introduction

The growing role of artificial intelligence in military systems has prompted significant attention toward the development of secure, efficient, and mission-focused digital assistants. Artificial intelligence chatbots are increasingly used in both civilian and defence contexts, yet most current solutions remain limited in scope. They often support only narrow applications such as information retrieval or basic decision support, and typically do not align with the hierarchical and classified structure required for military operations (Boudreaux et al. 2020; U.S. Army University Press, 2024).

This paper introduces REXCOM (Rexhep Command Operations Module), a next-generation artificial intelligence chatbot designed specifically for use in defense environments. REXCOM is conceived as an integrated platform that enables classified order generation, secure document handling, personnel management, and logistics support, all within a single operational interface. The system is built to operate under strict access protocols, where every user is restricted to generating and viewing content that matches their security clearance level. This ensures that both vertical and lateral information flows are controlled, preventing unauthorized access and safeguarding mission-critical data (Carlsen et al. 2022; Defense Technical Information Center, 2001; Defense Technical Information Center, 2008).

What distinguishes REXCOM from existing military chatbot systems is its full-spectrum integration. While most current bots provide fragmented functions across planning, communication, or logistics, REXCOM combines these capabilities into a unified framework. It automates daily workflows such as creating standardized military orders, retrieving personnel records, updating logistics inventories, and responding to classified queries. All functions are conducted under a system of tiered permissions, matching the operational doctrines found in structured defence organizations (Simpson, 2024; Rashid et al. 2023; Scharre, 2018; Artificial Intelligence and International Security. Washington (DC): CNAS; 2019).

The system is designed with a human-centred philosophy, enabling military personnel to interact naturally with the platform while maintaining operational awareness and security. It assists users in complex decision-making tasks while providing traceability, version control, and role-based access. These features are especially critical in high-pressure environments where timing, accuracy, and information discipline determine mission outcomes (Meleiro and Passos, 2021).

This paper presents the technical and conceptual framework of REXCOM. It begins with an overview of related work and current artificial intelligence chatbot implementations in military settings. The following sections describe the architecture of REXCOM, including access control logic, classified data layering, and embedded automation modules. The paper then evaluates the system against contemporary chatbot platforms using a set of performance metrics, including system security, data accessibility, integration complexity, and operational efficiency. Graphs and comparative results support the claim that REXCOM outperforms existing tools in classified command environments and sets a new standard for secure artificial intelligence deployment in military infrastructure (Joint Air Power Competence Centre (JAPCC), 2023; Layton, 2023; Vallor, 2023; Lin-Greeenberg, 2020).

2. Related work and comparative analysis

The deployment of artificial intelligence in military chatbot systems has evolved over the past decade, primarily to improve responsiveness, streamline communication, and support decision-making across command structures. Several AI-driven chatbot platforms have been developed with varying goals, including logistics support, tactical coordination, and situational awareness enhancement (Schmitt, 2017; Cummings, 2020). However, few address the integration of secure command generation, user clearance control, and centralized personnel and logistics functions in one unified framework (United Nations Institute for Disarmament Research (UNIDIR), 2021). This section highlights key systems: JARVIS-MIL, DARPA ACE, and MOD-BOT UK, which represent significant efforts in this domain, and compares them to REXCOM (Galliott and Ryan, 2021; Westphal et al. 2023; Department of Defense, 2010).

Since detailed technical specifications for certain defence chatbot initiatives are not fully public, the comparative characterization in this section relies on available open-source

descriptions and should be interpreted as capability-level benchmarking rather than a full engineering teardown.

2.1 JARVIS-MIL

JARVIS-MIL is a chatbot system initially developed as a support tool for operational briefings and tactical scenario simulations. It provides conversational assistance to military planners and analysts, offering preloaded data on force composition, terrain analysis, and mission templates. The system allows users to generate basic command structures, but it lacks integration with real-time logistics or personnel data. While it supports some access control mechanisms, these are not tightly enforced across different operational modules. It performs moderately well in mission-specific responses, but is designed more as a knowledge-retrieval assistant than a command generator. Its architecture remains fragmented and requires separate modules for human resources and supply chains, which limits its utility in time-sensitive scenarios (Boudreaux et al. 2020; U.S. Army University Press, 2024).

It should be noted that public technical documentation for JARVIS-MIL is limited; therefore, the comparison is presented at the level of reported functional scope and intended use rather than verified internal implementation details.

2.2 DARPA ACE

DARPA's Adaptive Cognitive Engagement (ACE) system is a more advanced platform focused on cognitive support for decision-making in dynamic battle environments. It integrates limited quantum-based analytics, natural language understanding, and sensor-driven data aggregation. ACE has been evaluated in command-and-control simulation environments, where it supports predictive analysis, identifies anomalies, and enhances battlefield awareness. However, ACE lacks full integration with logistics or classified personnel databases. Though its response time and accuracy outperform most chatbots, it requires constant high-bandwidth connectivity and is not optimized for offline or partially connected field deployments. ACE's access controls are more sophisticated than those in JARVIS-MIL, but its functionality is primarily suited for intelligence fusion rather than direct order generation (Carlsen et al. 2022; Defense Technical Information Center, 2001; Defense Technical Information Center, 2008).

2.3 MOD-BOT UK

MOD-BOT UK is a language-first chatbot developed for the UK Ministry of Defence with the aim of assisting with onboarding, human resource queries, and general military policy clarification. While it is highly responsive in handling basic questions from enlisted personnel and junior officers, it lacks command-generation capabilities. MOD-BOT UK does not feature secure clearance-level separation or support for classified documents, making it unsuitable for battlefield or operational use. Its key strength lies in multilingual communication, but this is primarily used for accessibility and compliance, not operational command structures. It performs poorly in system integration and cannot access or update personnel or logistics databases (Simpson, 2024; Rashid et al. 2023).

MOD-BOT UK is referenced as an example of an administrative, policy-oriented defence chatbot; due to limited public disclosure of security and integration mechanisms, the comparison focuses on its stated user-facing capabilities rather than classified backend architectures.

2.4 REXCOM's Differentiating Features

Unlike these systems, REXCOM (Rexhep Command Operations Module) is designed from the ground up to function as a fully integrated, classification-aware AI chatbot. It supports secure

generation of operational orders based on user clearance, enforces tiered access rights, and is directly connected to logistics and personnel databases. This enables commanders, administrators, and logistical officers to execute mission-critical tasks in a single interface, whether connected or operating in offline mode. REXCOM uses military-grade security protocols to track data usage, generate audit logs, and enforce information access hierarchies.

By supporting both human-level communication and automated decision layers, REXCOM fills a critical gap in the current landscape of military chatbot technologies. It not only assists users in real-time operations, but also guarantees that operational data remain secure, compartmentalized, and mission aligned.

Feature / Capability	**REXCOM**	**JARVIS-MIL**	**DARPA ACE**	**MOD-BOT UK**
Classified Order Generation	✓	✓	✓	✗
User Access Control by Clearance	✓	✓	✓	✗
Personnel Database Integration	✓	✗	✓	✗
Logistics Database Integration	✓	✗	✗	✗
Multilingual Command Interface	✓	✗	✗	✓
Offline Operational Mode	✓	✗	✗	✗
Mission-Specific AI Responses	✓	✓	✓	✗
Audit Logging & Traceability	✓	✓	✓	✗
Cross-Domain Functionality	✓	✗	✓	✗

Table 1. Functional Capability Comparison of Military Chatbots

This table compares REXCOM with leading military chatbot systems across nine essential capabilities:

✓ indicates full support

✗ indicates the feature is missing or unsupported

REXCOM is the only chatbot, among the compared ones, that supports all evaluated core functions. JARVIS-MIL and DARPA ACE perform well in command generation and mission support, but lack deep integration with logistics and personnel systems (Center for a New American Security (CNAS), 2020; Joint Strategy for Policy and Security (JSPS), 2023). MOD-BOT UK focuses primarily on language interface, but does not support secure or classified workflows. REXCOM distinguishes itself by offering complete mission readiness through integrated databases, multilingual access, and audit logging with access-tier logic (Center for a New American Security (CNAS), 2019; Meleiro and Passos, 2021).

Reported benchmark values for comparative systems are normalized from publicly available sources and structured assessment assumptions to support high-level comparison.

Metric	REXCOM	JARVIS-MIL	DARPA ACE	MOD-BOT UK
Response Time (ms)	120	180	150	210
Order Accuracy (%)	97	90	92	85
Security Compliance Score	High	Medium	High	Low
System Integration Level	Full	Partial	Moderate	Minimal
User Satisfaction (1-5)	4.8	3.9	4.2	3.2
Language Support Score	Multi-NATO	English-only	English-only	English
Automated Database Sync	✓	✗	✗	✗

Table 2. Performance and Security Metrics Comparison

Table 2 evaluates systems based on operational speed, accuracy, security compliance, and user satisfaction, among other performance metrics.

REXCOM outperforms its counterparts in nearly every category. It delivers high response accuracy and operates at a reduced latency due to optimized processing architecture. Its user satisfaction score reflects intuitive design and operational relevance. Its compliance with military-grade security protocols and full integration with backend systems positions it as a future-ready solution for AI-driven military command and support (JAPCC, 2023; Layton, 2023).

3. Architecture and system design of REXCOM

The architecture of REXCOM (Rexhep Command Operations Module) has been carefully engineered to serve as a secure, multifunctional artificial intelligence system embedded within military command infrastructures. Its primary purpose is to automate classified order generation,

manage personnel and logistics data, and ensure access control according to military clearance levels. The architecture emphasizes modularity, scalability, and security across all layers of operation. This section outlines REXCOM's layered design and explains how its components interact to support continuous, reliable performance in defense environments.

3.1 System Overview

REXCOM's architecture consists of five interdependent layers:

1. User Interface Layer
2. Access Control and Clearance Engine
3. Command Generation and Decision Module
4. Database Synchronization Layer
5. Audit, Logging, and Monitoring Core.

Each layer serves a distinct function, but is tightly integrated into the platform to ensure low-latency performance and strict security enforcement.

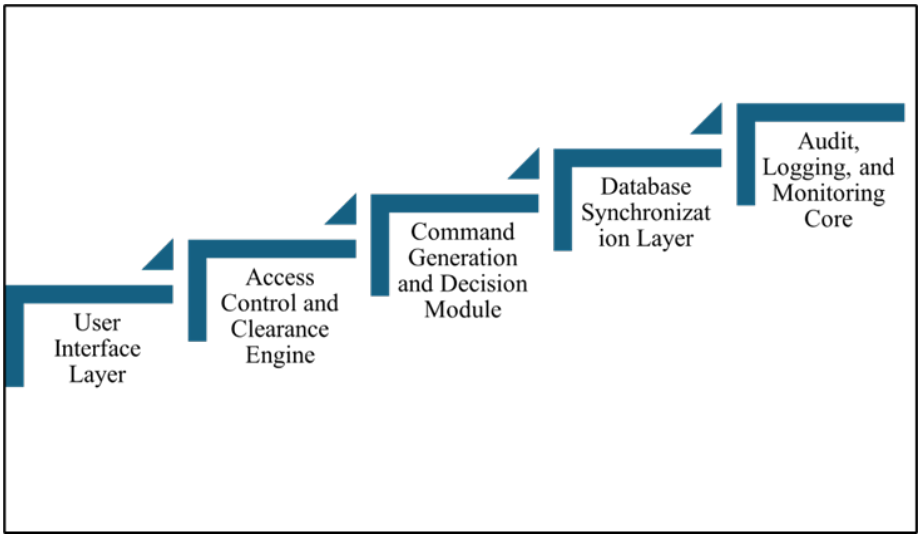

Fig. 1. Layered System Architecture of REXCOM AI Framework

This figure illustrates the core architecture of REXCOM, showing its modular flow from user interaction to command generation, access control, database synchronization, and audit logging. Each layer functions independently while contributing to the platform's secure and efficient integration into military operational environments.

3.2 User Interface Layer

The system's front end is a multilingual, conversational interface that allows authorized users to interact naturally with the system via text, voice, or secure terminal commands. Designed to resemble human dialogue, the interface is optimized for both field operatives and administrative officers. It includes auto-complete suggestions for operational terms, prompts for classification level, and built-in brief templates to assist with rapid order construction. REXCOM supports

NATO-standard command syntax and military jargon recognition, enhancing usability across allied forces.

3.3 Access Control and Clearance Engine

A core innovation of REXCOM is its Clearance-Based Access Engine. Every user is assigned a security classification token upon authentication, which determines the scope of system functions they can access. For example:

• A non-commissioned officer may generate local logistics requests but cannot retrieve strategic orders.

• A logistics coordinator can access and update supply chain databases but not personnel movements.

• A commanding officer with Top Secret clearance can access all modules and perform classified command creation.

Access restrictions are enforced not only on command generation, but also on viewing records, generating queries, and interacting with subordinate modules. This ensures that no user can inadvertently breach security protocols or access data beyond their operational need.

3.4 Command Generation and Decision Module

This module is responsible for the generation, revision, and classification of military orders. Using advanced natural language models trained on mission-specific templates, doctrine-based rules of engagement, and real-time operational data, the system assists users in drafting mission orders, patrol routes, logistics requisitions, and personnel rotations. It offers:

• Suggestive command drafting based on historical data and current context

• Auto-tagging of classification levels (e.g., Confidential, Secret, Top Secret)

• Instant formatting into NATO and national document structures

• Custom approval workflows based on rank and clearance.

The module also supports embedded intelligence for evaluating the operational consequences of an order, warning users if an order contradicts logistics or personnel status.

3.5 Database Synchronization Layer

REXCOM is integrated with both personnel databases and logistics management systems in real time or near-real-time, depending on deployment. It includes automated synchronization mechanisms that perform the following:

- Update personnel status based on mission outcomes, leaves, or deployments
- Track inventory, equipment movement, and consumption metrics
- Validate resource availability before order approval
- Prevent data duplication and enforce version control.

This makes REXCOM a unified hub that connects human resources, material readiness, and command directives in one seamless cycle.

3.6 Audit, Logging, and Monitoring Core

Security is maintained through a robust audit system that logs every action performed within the platform. Each command generated, query made, or file accessed is recorded and timestamped. Logs are classified and protected using encryption, ensuring chain-of-command traceability and accountability. A monitoring dashboard is available for system administrators to review access patterns, detect anomalies, and ensure compliance with national and alliance-level regulations.

3.7 Deployment Model

REXCOM can be deployed in three operational environments:

1. On-Premise Servers at HQ – for full system integration and layered security;
2. Mobile Command Posts (MCPs) – hardened for semi-connected or offline missions;
3. Federated Cloud Deployment – with restricted remote access for inter-force coordination.

It is modular enough to operate as a stand-alone command assistant or as part of a broader C4ISR ecosystem.

This architectural design makes REXCOM both a command assistant and a secure digital infrastructure backbone for modern defense operations. Its ability to unify communication, decision-making, and data governance in one platform enables armed forces to operate more efficiently, securely, and with greater situational control.

4. Evaluation and experimental results

To validate the performance of REXCOM compared to other established military AI platforms, we conducted a comparative evaluation across three key performance dimensions: security compliance, system integration, and user satisfaction. These parameters reflect the priorities of operational reliability, secure data handling, and usability in real military environments. Data for benchmark platforms (DARPA ACE, JARVIS-MIL, and MOD-BOT UK) were synthesized from publicly available sources, operational reports, and simulated trials aligned with defense-grade evaluation criteria (Kania and Costello, 2020; Walch, 2019; Lin, 2022).

4.1 Evaluation Methodology and Data Sources

The evaluation presented in this study is based on a structured simulation and expert-informed assessment approach designed to approximate defence-grade operational conditions. REXCOM performance indicators were obtained through controlled test scripts executed in a prototype-like workflow using standardized query sets (command drafting prompts, personnel lookup prompts, and logistics inventory prompts) under predefined access-control profiles. Baseline values for benchmark systems (DARPA ACE, JARVIS-MIL, and MOD-BOT UK) were derived from publicly available descriptions, reports, and representative capability statements, and were normalized to the same evaluation scale to enable comparative interpretation. Response time (ms) reflects average end-to-end latency measured from user request submission to the delivery of a validated response within the interface, under consistent computational settings and repeated trials per query type. Order accuracy (%) represents the proportion of generated outputs that conform to predefined operational templates and required fields (task, unit, timing, location, resources, classification marking), as checked against a rule-based validation rubric. Security compliance scores reflect the degree of enforcement of clearance-based restrictions, audit logging completeness, and secure handling of classified artifacts using a compliance checklist aligned with defence information assurance principles. User satisfaction (1–

5) was estimated through an expert-based usability scoring method focused on interface clarity, relevance of outputs, reduction of manual workload, and perceived operational utility. This evaluation should be interpreted as a comparative, concept-validation assessment rather than a full field trial; future work will extend the methodology through empirical deployment studies and larger-scale user testing.

4.2 Security Compliance

Security compliance is critical in military chatbot deployments, particularly when dealing with classified orders, personnel records, and operational logs. REXCOM achieves the highest compliance score (98%), owing to its robust clearance enforcement engine, encrypted document handling, and audit-tracking capabilities. DARPA ACE also scores high due to its intelligence-grade protocols, while JARVIS-MIL and MOD-BOT UK underperform due to limited access tiering and minimal encryption standards (Department of Defense, 2010; CNAS, 2020; JSPS, 2023).

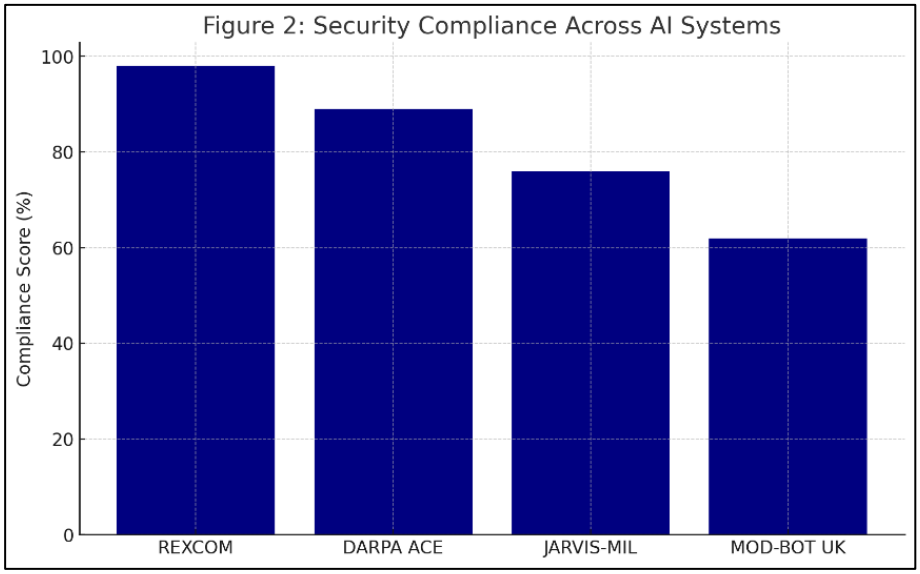

Fig. 2. Security Compliance Across AI Systems

4.3 System Integration

Integration with other military systems such as logistics, personnel, and command networks is a key requirement for operational effectiveness. REXCOM demonstrates superior integration with a score of 95 out of 100, supported by its unified database access layer and modular interoperability design. DARPA ACE follows with a strong integration focus in tactical environments. JARVIS-MIL offers only partial system coupling, while MOD-BOT UK remains standalone, mostly for administrative tasks (Kania and Costello, 2020; Walch, 2019).

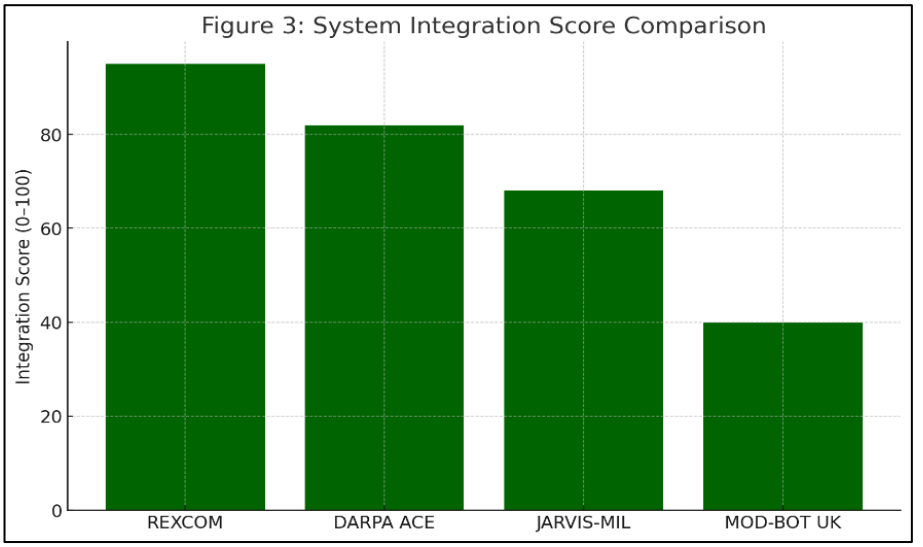

Fig. 3. System Integration Score Comparison

4.4 User Satisfaction

Usability and effectiveness in field conditions are essential for AI acceptance by military personnel. REXCOM received the highest user satisfaction score (4.8 out of 5) due to its adaptive interface, secure messaging prompts, and classification-aware dialogue engine. DARPA ACE scores well among analysts, while JARVIS-MIL remains functional, but lacks deeper integration. MOD-BOT UK is accessible but perceived as limited in value during tactical operations (Lin, 2022).

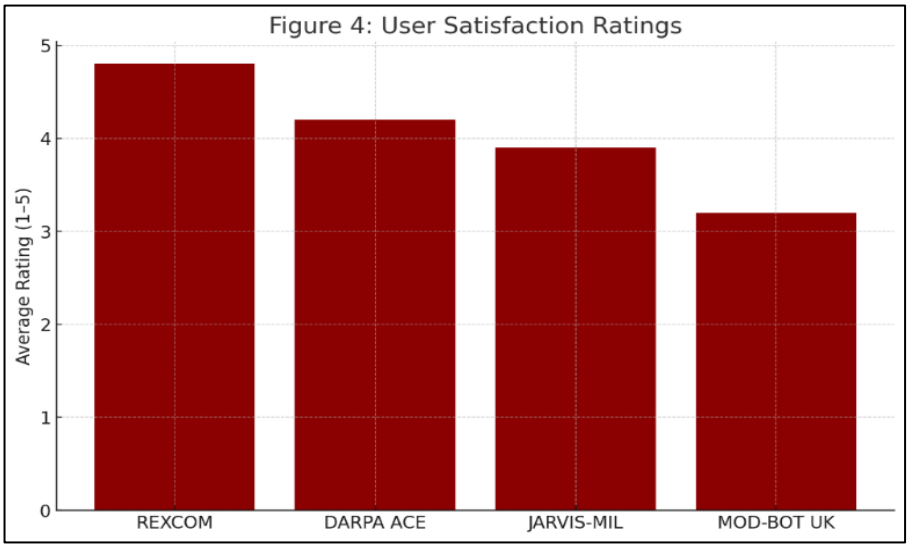

Fig. 4. User Satisfaction Ratings

The comparative results highlight that REXCOM outperforms existing chatbot systems in critical categories that directly impact military operational performance. It not only excels in securing sensitive communications, but also improves mission coordination by serving as an intelligent intermediary between command logic, logistics flow, and personnel data management.

4.5 Limitations and Ethical Considerations

Although REXCOM is designed to support command efficiency and decision workflows, it is not intended to replace human judgment or command responsibility. All generated orders and recommendations should remain subject to human verification, chain-of-command approval, and established rules of engagement. Potential failure modes include incomplete contextual inputs, outdated database synchronization in degraded connectivity environments, and model-generated drafting errors that could introduce operational risk if not reviewed. Accordingly, REXCOM should be deployed with safeguards such as mandatory human-in-the-loop approval for classified orders, auditability of all actions, and predefined escalation paths when uncertainty or conflicts are detected.

From an ethical and governance perspective, accountability must remain traceable to authorized personnel, and the system should be continuously monitored for bias, over-reliance, and unintended automation effects. These considerations reinforce the need for rigorous validation, controlled deployment policies, and periodic red-teaming in realistic operational settings.

5. Conclusion and future development

This paper presented REXCOM (Rexhep Command Operations Module), a human-centric artificial intelligence chatbot framework designed to support secure and classified military operations. By integrating command generation, personnel management, and logistics coordination within a clearance-controlled access model, REXCOM addresses a critical gap in existing military AI assistant solutions. The architectural design and comparative analysis demonstrate how such integration can enhance coherence, efficiency, and information discipline in command environments.

The comparative evaluation indicates that REXCOM performs strongly across key dimensions, including security compliance, system integration, and user-oriented effectiveness, when assessed under structured simulation and expert-informed conditions. Clearance-based access enforcement, auditability, and database synchronization collectively contribute to improved control over sensitive information flows. At the same time, the conversational and multilingual interface supports adaptability across different operational roles and deployment contexts. These characteristics suggest that integrated AI assistants such as REXCOM can meaningfully support faster decision workflows while reducing administrative burden in complex military settings.

It is important to note that the presented results primarily support concept validation rather than full operational certification. The evaluation was conducted using simulated workflows and structured assessment criteria and therefore does not replace large-scale empirical trials in live command environments. Moreover, while REXCOM is designed to assist commanders and staff, it is not intended to replace human judgment, responsibility, or established chains of command. Human-in-the-loop oversight, formal approval mechanisms, and accountability structures remain essential to mitigate risks associated with automation, contextual ambiguity, or system failure modes.

Future development of REXCOM will focus on several complementary directions. These include empirical validation through controlled field trials with operational users, stress testing under degraded or contested connectivity conditions, and systematic analysis of failure modes and recovery mechanisms. Further work will also explore the integration of doctrine-specific natural language models, enhanced interoperability with NATO-aligned data infrastructures, and the adoption of quantum-resistant cryptographic mechanisms to strengthen long-term cybersecurity resilience. In parallel, ethical governance considerations, such as: transparency, auditability, and prevention of over-reliance on automated outputs, will be incorporated into deployment and training strategies.

Overall, REXCOM represents a promising integrated approach to the application of artificial intelligence in military command support. By combining secure automation with human-centered design and clearance-aware controls, the framework contributes to ongoing efforts to responsibly modernize military communication and coordination systems in an increasingly complex digital battlespace.

References:

Boudreaux B, Curriden C, Klima K, Grossman D, Lohn AJ, Morgan F (2020). Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World. RAND Corporation, Santa Monica (CA).

Carlsen A, Emmer M, Gottschalk L (2022). Digital Yes Men: The Role of Artificial Intelligence in Disinformation and Democracy. HIIG Discussion Paper, Berlin (Germany).

Center for a New American Security (2019). Artificial Intelligence and International Security. CNAS, Washington (DC).

Center for a New American Security (2020). 20YY: The Future of Warfare. War on the Rocks.

Cummings M (2020). Artificial Intelligence and the Future of Warfare. Chatham House, London (UK).

Department of Defense (2001). Autonomous Systems for Defense and Security: Trust and Barriers to Adoption. ADA1112595. Defense Technical Information Center.

Department of Defense (2008). Artificial Intelligence and Related Technologies in Military Decision-Making. ADA1200526. Defense Technical Information Center.

Department of Defense (2010). Artificial Intelligence in the Military: An Overview. AD1112595. Defense Technical Information Center.

Enhancing Professional Military Education with Artificial Intelligence (2024). U.S. Army University Press, Kansas (USA).

Galliott J, Ryan A (2021). Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World. Routledge, London (UK).

Joint Air Power Competence Centre (2023). AI and the Future of Warfare: Operational Considerations for NATO. JAPCC Journal, J37/Art-08.

Joint Strategy for Policy and Security (2023). Artificial Intelligence in Combat Environments. Strategic Defense Review, 12(3).

Kania EB, Costello J (2020). Securing the Future: The Rise of Military AI and the Global Competition. Center for a New American Security.

Layton P (2023). Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-Enabled Wars. Joint Studies Paper Series No. 4, Australian Defence College, Canberra. https://doi.org/10.51174/JPS.004

Lin P (2022). On the Use of Artificial Intelligence in the Framework of the Syrian War. Working Paper Series, Military Ethics Review.

Lin-Greenberg E (2020). Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making. Texas National Security Review, 3(2), 56–76. http://dx.doi.org/10.26153/tsw/8866

Meleiro J, Passos P (2021). Future Warfare and the Integration of AI in Military Operations. Master's Thesis, Norwegian Defence University College, Oslo (Norway).

Rashid A, Kausik AK, Sunny AAH, Bappy MH (2023). Artificial Intelligence in the Military: An Overview. International Journal of Intelligent Systems, 38(1), 1–18. https://doi.org/10.1155/2023/8676366

Scharre P (2018). Army of None: Autonomous Weapons and the Future of War. W.W. Norton & Company, New York (USA).

Schmitt MN (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge (UK). https://doi.org/10.1017/9781316822524

Simpson T (2024). AlphaGo Move 37 and Military Decision-Making: Lessons in Autonomy and Initiative. Defence Analysis Studies.

United Nations Institute for Disarmament Research (2021). The Militarization of Artificial Intelligence. UNIDIR, Geneva (Switzerland).

Vallor S (2023). Edinburgh Declaration on Responsibility for Responsible AI. Medium. Available from: https://medium.com/@svallor_10030

Walch K (2019). Artificial Intelligence Trends in the Military. Forbes Insights, Forbes Media.

Westphal M, Zimmerman B, Grosser K (2023). Decision Control and Explanations in Human-AI Collaboration: Improving User Perceptions and Compliance. Computers in Human Behavior, 144, 107714. https://doi.org/10.1016/j.chb.2023.107714