Opportunities and Constraints in Applying Artificial Intelligence in Military Enterprise

Juha Mattila and Simon Parkinson

Introduction

Artificial Intelligence (AI) stands out as a new magical way to transform the digital age to further heights [1]. How can we assess the readiness of military enterprise in adopting or innovating new capabilities enhanced by the AI related technologies?

The short paper uses an enterprise architecture (EA) tool developed specially for military enterprises to assess the opportunities and challenges in adapting the benefits of AI. The EA tool analyses the strategic posture and operational processes of a military force [2]. Furthermore, it focuses primarily on the command and control related capabilities including sensemaking, decision making, and organisational learning. Additionally, the tool helps to analyse the readiness of information, security and technical structures of armed forces.

Theory and literature survey

Using Thorpe et al.'s [3] view of the evolution of business knowledge, Mattila and Parkinson define the evolutionary roadmap for strategic posture in confrontation and doctrinal improvement [2], command and control [4], and military information management [5]. The supporting technical layers of information security [6] and ICT infrastructure [7] are studied correspondingly and combined in the framework [8]. The EA tool merges the above layers and defines the forces acting within the structure presented in Figure 1.

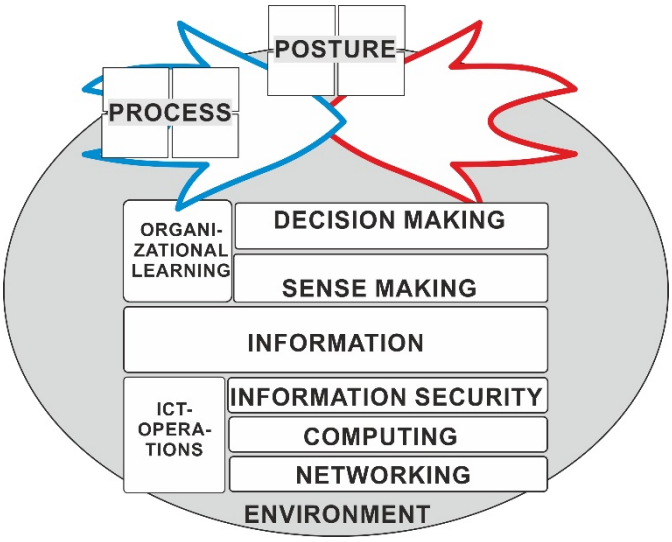

Figure 1: Military enterprise structure from enterprise architecture viewpoint.

A literature survey was made to create an understanding of the current opportunities and challenges that enterprises feel they are facing when considering improving their business

with AI enhanced features. The survey was done as document research [9, pp. 29-33] explained in Table 1.

Table 1: Parameters of the literature survey on AI implementation

Literature survey	Quantity	Quality
Sources	27	news articles to academic research; commercial companies to governmental agencies
Found opportunities and challenges = concerns	21	May indicate that there are not many practical implementations yet.
Hit volume from 27 sources	216	May indicate similar viewpoints
Concerns were arranged in categories:	4	In which the following concerns gained the most hits:
- Culture	31%	regulations and governance; security, safety, and privacy; organisational adaptation
- Process	27%	lack of competency; difficulties in explaining the results of AI logic
- Data	30%	acquiring feasible data; biased data and algorithms
- Technology	12%	narrow nature of current AI

The four areas of AI opportunities and challenges and their eight key issues create the performance metrics for the EA tool in the following section.

Research

The literature review provides a statistical data concerning opportunities and challenges in applying AI in any enterprise. The collected AI data is projected to a case study [10] of an anonymous Armed Forces (Blue Force) C4I structure and its intended improvement. The feasibility of the EA tool is measured by its ability to anticipate the accelerators and obstacles in the journey of AI implementation.

The Blue Force illustrated in Figure 3 seems to be gaining an advantage against their adversaries from the evolutionary posture since it has been acquiring the modern armament steadily. There may, however, be a tendency towards the operational posture as the cost of contemporary armament is rising and the available workforce is diminishing.

The Blue Force strategy for military process performance seems to be on a path towards coordination aiming for joint force capabilities. Subsequently, there are also indications towards unified logistics and replicated force generation.

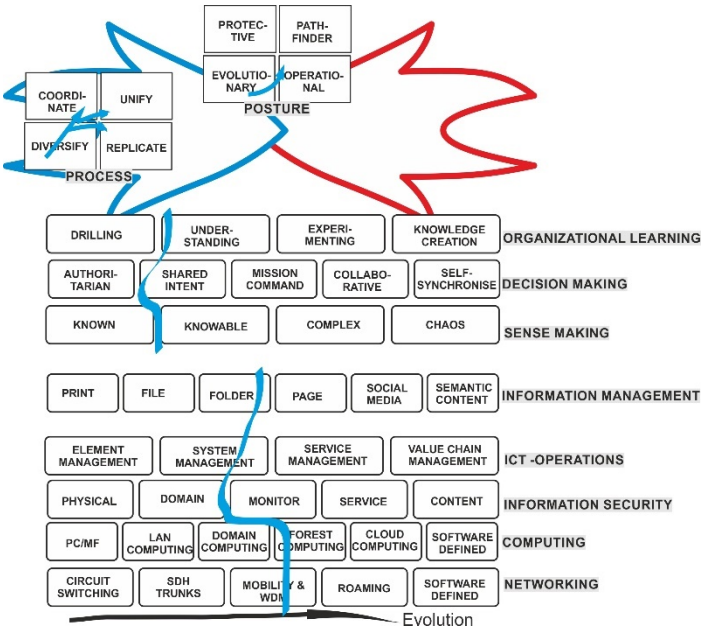

Figure 3: Case of Blue Force in aiming to apply AI

The essential parts of the Blue Force command and control capabilities are based on learning by drilling and somewhat by understanding. Furthermore, the Blue Force decision making has an authoritarian approach with a touch of shared intent. The sensemaking seems to focus on the areas of known and knowable.

The information management of the Blue Force is somewhere between folder and page management, and the information security is mainly based on controls within each domain. There seem to be advanced bandwidth and mobility services available, whereas computing seemed decentralised and connected no further than forest level. ICT operations seem to be at system management level.

Results and discussion

The specific concerns in AI implementation into generic enterprises are reflected against the results of analysis of the Blue Force enterprise structure. Table 2 is illustrating this reflection either positive, i.e., opportunity or negative, i.e., challenge. The direct guidance is either utilising the opportunities or trying to mitigate the challenges in coming AI implementation within the Blue Force.

Table 2: Testing the EA tool in analysing opportunities and challenges in applying AI within the Blue Force

Area of concern	Key issues in applying AI	Reflection in the analysis of the Blue Force with EA tool	Recommendations for AI implementation in the Blue Force
Culture	Regulation, Governance	+ Aiming for operational advantages helps if AI implementation is measured by performance improvements. + Joint operations capabilities will support the AI focus on coordinated and unified features.	Assign performance indicators aligned with the development strategy. Focus on end-to-end process performance to overcome the sub-optimisation.
	Security, safety, and privacy	- Folders and domain borders will hinder the access to data needed for AI (ID).	Focus on smaller areas to use AI to mitigate constraints. Data governance needs to be improved to gain better access to existing data.
	Organisational adaptation	+ Authoritarian decision-making favours a top-down implementation. - Organisational learning will slow down the execution.	High-level business cases will help to gain top-level stakeholders buy-in. An implementation may need a stronger consulting arm.
Process	Competency	+ Authoritarian decision-making and drilling learning favour building new competencies top-down (ID). + Linear and short processes favour short-term performance goals.	Improve the understanding of leading management. Make goals short and meaningful for higher management. Emphasise top-down change management.
	Explaining AI logic	+ Sense-making in known and knowable areas helps to ratify the outcome of AI.	Start with simple regression analysis and build towards more complex analysis. Trust needs slow building.
Data	Acquire more data	- Distributed and stove-piped data slow down the data acquisition.	Keep AI projects small to achieve faster results.

			Consider using synthetic data.
	Bias in data and algorithms	- Acquisition of data volume needed for neural networks will be challenging from distributed, and domain defined computing (ID).	Applying AI where data integrity and volume are sufficient or acquirable. Need to build ownership of data, data sharing and a better base for trusted security.
Technology	Narrow nature of AI	+ It will be easier to start with improving existing manual functions in broad approach(ID).	Consider using enterprise and public AI as a service to accelerate the development.

The EA tool supports the analysis of enterprise from cultural dimension down to technical dimensions covering the indicated areas of concern in AI implementation. Therefore, the EA tool is sufficiently holistic in modelling the military enterprise structure.

The reflection of architectural analysis of the Blue Forces enterprise structure against eight key issues in AI implementation provides the enterprise architect with ten opportunities to accelerate the adaptation of AI and recognises four challenges requiring mitigation. Consequently, the EA tool recognises both driving and hindering forces within an enterprise.

The EA tool identified four inter-layer dependencies (ID) in implementing AI. Consequently, the EA tool recognises inter-dependencies through the enterprise structure compared to layer-oriented models.

References

[1] M. Chui, M. James, M. Miremadi, N. Henke, R. Chung, P. Nel and S. Malhotra, "Notes from the AI frontier - Insights from hundreds of use cases," McKinsey Global Institute, 2018.

[2] J. Mattila and S. Parkinson, "Evolution of military enterprise from architecture viewpoint," in *International Society of Military Sciences 2017*, Oslo, 16.November 2017, 2017.

[3] R. Thorpe, O. Jones, A. Macpherson and R. Holt, "The evolution of business knowledge in smaller firms," in *The evolution of business knowledge*, H. Scarbrough, Ed., Oxford, Oxford University Press, 2008, pp. 23-49.

[4] J. Mattila, "Military Knowledge Management: Sense-making, decision-making and knowledge creation," in *Proceedings of the 17th European Conference on Knowledge Management 1-2.9.2016 Ulster University*, Belfast, 2016.

[5] J. Mattila and S. Parkinson, "Evolution of military information management," *National Defence University Scientific Quarterly, Poland,* no. 105 (4), 2016.

[6] J. Mattila and S. Parkinson, "Evolution of military information security," in *Proceedings of the 16th European Conference on Cyber Warfare and Security ECCWS 2017 University College Dublin Ireland 29 - 30 June 2017*, Dublin, 2017.

[7] J. Mattila and S. Parkinson, "Predicting the architecture of military ICT infrastructure," in *Proceedings of the 11th European Conference on Information Systems Management 14-15 September 2017*, Genoa, 2017.

[8] J. Mattila and S. Parkinson, "Enterprise architecture as a tool in military change management," in a *6th international conference on management, leadership and governance, 24 - 25. May*, Bangkok, 2018.

[9] A. Dresch and D. Antunes, Design science research, Cham: Springer International Publishing, 2015.

[10] D. Remenyi, Case study research, Reading: Academic Conferences and Publishing International, Ltd., 2012.