OPEN PUBLICATIONS

Metaverse: A Tool for Improving Air Commander and Staff Skills

Volume 9, Number 4, 2024

ISSN 2957-7160 (Online)
ISSN 2957-7799 (Print)

Let us know your thoughts on
"Metaverse: A Tool for Improving Air Commander and Staff Skills"
by emailing us at: ***editor@openpublications.org***
www.openpublications.org

CREDITS

CONTRIBUTING AUTHOR

Ms Kristine Kvam,
CTO at Fynd Reality AS

OPEN CAPABILITY LEADER

Col Stefan Lindelauf

OPEN MANAGING EDITOR

Dr Mehmet Kinaci

OPEN OPERATIONS MANAGER

LtC Alexios Antonopoulos

ACTION OFFICER

LtC David Casado Martinez

OPEN EDITORIAL REVIEW BOARD

LtC Ferenc Pasztor
LtC Tor-Erik Hanssen
Cdr Silvio Amizic
Cdr Alban Morel
Cdr Alan Cummings
LtC Dirk Mathes
Maj Mithat Almaz
Mr Helmar Storm
Ms Klodiana Thartori

TECHNICAL EDITOR

Dr Maureen Archer

ART DESIGNER

PO1 Isabel Wences

CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

This paper explores how the metaverse can be a supporting framework for the adoption of Emerging and Disruptive Technologies (EDTs), using the case of improving Air commander and staff skills to substantiate the discussion. The metaverse is defined as an intertwining of our physical and digital lives in the form of a seamless flow between what we see and interact with physically and a virtual environment; it is a persistent, virtual space where people share simultaneous experiences from remote physical locations.

The metaverse is proposed as a tool for the training and education of Air commanders and staff, as well as a hub for after-action reviews and recommendations for further training. With the right input, the metaverse can facilitate simulations of courses of action (COAs) to foster learning, with all participants in separate locations.

Due to the nature of the metaverse as a convergence of several interconnected systems with distribution as one of its main advantages, security concerns rise as a part of the discussion. Secure connectivity is a requirement, and with Artificial Intelligence (AI) integration, resilience to adversarial attacks and perturbation of data will be key for secure use of the metaverse.

The adage "train as you fight, fight as you train" can, with wargaming in the metaverse (see Figure 1 showing a concept illustration of a 3D wargaming map), become a reality. The metaverse can be the facilitator and designer of situations, giving teams the possibility to test different strategies and COAs against a virtual Red team and seeing them play out with different enemy COAs in response, all visualized in 3D. In an educational setting, the metaverse offers the same flexibility as it does to wargaming, but adds strategies like nano-, experiential-, and game-based learning.

Based on these challenges, the paper offers the following recommendations for NATO. Acceptance of the metaverse must be cultivated throughout the organization, and the use of its underlying technologies must be proven beneficial. The key recommendation of this paper is therefore to think of any integration in two distinct phases, starting early with the simpler and most clear-cut use cases while preparing for a more holistic integration to maximize the benefits the metaverse offers.

In the short term, the metaverse should be used as a semi-integrated learning and training system. As an arena for distributed procedure training, it could prove a cost-effective starting point, highlighting for decision makers the cost saved on trainer and trainee travel, minimized equipment attrition, and increased course content retention. Cost-effective procedure training, availability of 3D models of equipment, and motivation and game-based learning are key activities in the short term.

In the longer term, the metaverse should let an educator use a planning interface to recommend training templates for different groups of trainees, based on previously completed training, experiences from previous real operations, and wargaming exercises. An editor function should allow the educator to customize the scenarios. In those cases where the trainees benefit from adversarial training, the educator should be able to define the capabilities of a virtual Red team with opposing COAs during training. Disaggregated integration, adversarial method competency, and anthropocentric[1] AI are key activities in the longer term.

[1] *"Interpreting or regarding the world in terms of human values and experiences", Merriam-Webster, https://www.merriam-webster.com/dictionary/anthropocentric*

INTRODUCTION

Air superiority is not a luxury in war; it is the determining factor of victory, as Saunders and Souva conclude in their article Air superiority and battlefield victory (2020).

Emerging and disruptive technologies represent a pivotal tool for military training. Understanding its potential to enhance decision-making, coordination skills, and the leadership skills of Air commanders and staff is pressing for ensuring Air superiority in an ever-evolving global security landscape.

This paper explores how the metaverse can be a supporting framework for the adoption of EDTs with the goal of improving the skills of NATO Air commanders and staff.

The paper defines and describes the metaverse as a concept in itself and its use for NATO Air Command, as well as outlines the main security concerns associated with using the technologies of the metaverse in this context. The discussion moves on to take a closer look at two concrete use cases for skill elevation: a wargaming approach and the application of the metaverse in traditional, experiential, and blended learning strategies.

Following the main discussion, the paper concludes with a summary focusing on how the metaverse can be used as a training tool from the Air planning process to conducting Air operations. The summary contains recommendations for NATO and some key results and conclusions based on the discussions.

THE METAVERSE

This chapter outlines the prevailing descriptions of the metaverse and presents a definition for the purposes of the following discussions. Following the definition are two main points of interest, the first being how the metaverse can be used by NATO Air commanders and staff to increase skills and what the security concerns regarding such use are. The second point is looking closer at how learning and skill development can occur in the virtual environments of the metaverse.

DEFINITION

The term metaverse is a composite of the word universe and the Ancient Greek prefix meta-, which means with or after, or sometimes beyond, depending on the case (Wiktionary, 2023).

The term as we use it today was coined by author Neal Stephenson in 1992, in his novel Snow Crash. Though the book provides no specific definition of the metaverse, it is described as a persistent virtual world that reached, interacted with, and affected nearly every part of human existence in the book (Ball, 2022, p. 3).

The metaverse almost defies definition at present because it is more of an idea than a reality (Hackl, 2023, p. 7). Hackl defines it as the natural successor of today's mobile internet. Where web 1 connected information, which gave us the internet, and web 2 connected people, which gave us social media, web 3 connects people, places, and things, giving us the metaverse. According to Hackl, we are currently at the end of web 2 and the beginning of web 3 (Hackl, 2023, p. 8). Though many experiences can be based on audio and information sharing, there is a necessary visual output component to the idea of the metaverse, mostly in the form of 3D models and 3D data visualized within the virtual environment.

For this paper, the following definition is proposed:

The metaverse is an intertwining of our physical and digital lives in the form of a seamless flow between what we see and interact with physically and a virtual environment. The metaverse is a persistent, virtual space where people share simultaneous experiences from remote physical locations (Hackl, 2023, p. 8).

The early science fiction vision where the metaverse is a complete and separate world where humans live their lives in a simulation, is being replaced in literature and media by the reality where the metaverse takes the form of an intertwining of our physical and digital lives, supported by advances in Artificial Intelligence, machine learning and increased computing power.

This shift in perception and understanding of new technology, and its role in society and our daily lives, follows an easily recognizable path. The Gartner Hype Cycle (Figure 2) explains how these disruptive technologies evolve from early development to the enthusiastic belief that they will solve all problems, to the realization that they will probably not, and finally, to proper application where they can become a productive part of the relevant domains (Wikipedia, October 2023).

Media outlets, The Guardian and Business Insider[2]

[2] *Business Insider, 08 May 2023, https://www.businessinsider.com/metaverse-dead-obituary-facebook-mark-zuckerberg-tech-fad-ai-chatgpt-2023-5?op=1*

among others, proclaimed in early 2023 that "The Metaverse is dead"[3]. In the Gartner Hype Cycle framework, this negative opinion of the press indicates that the metaverse is currently past the peak of inflated expectations. Such pessimism of the layperson means that developers can continue their work without management and sales personnel pressuring for quick fixes and marketing stunts. The following sections will examine how the next stage in the Hype cycle (i.e. productive integration of the technology) might look.

DESCRIPTION

The metaverse, following the above definition, is at its core an agglomeration of the factors intelligent, interconnected, distributed, and digital, (I2D2), identified by the NATO Science and Technology Trends 2023-2043, Volume 1, as the heart of the strategy for a future agile and innovative Alliance with applied emerging, disruptive, and convergent technologies (Reding et al., 2023, pp. 11 - 13). In Figure 3, showing how I2D2 converge (Reading and Eaton, 2020. p. 8), the metaverse can be firmly placed in the middle of the Venn diagram.

Notably, the Intelligent factor is very much in the zeitgeist and at the heart of the metaverse. Without assuming that humanity will develop systems of general artificial intelligence or artificial consciousness, an integrated and integral AI that can explore large data sets, perform analyses and present a certain level of autonomous decision-making will be necessary to keep the metaverse relevant as a training arena. This futuristic vision notwithstanding, the existing models of machine learning and neural networks already present a considerable leap in development.

Neural networks are the cornerstone of modern machine learning, basing the deep learning algorithms on inspiration from biological processes. With access to data and with proper loss mechanisms programmed, the neural network

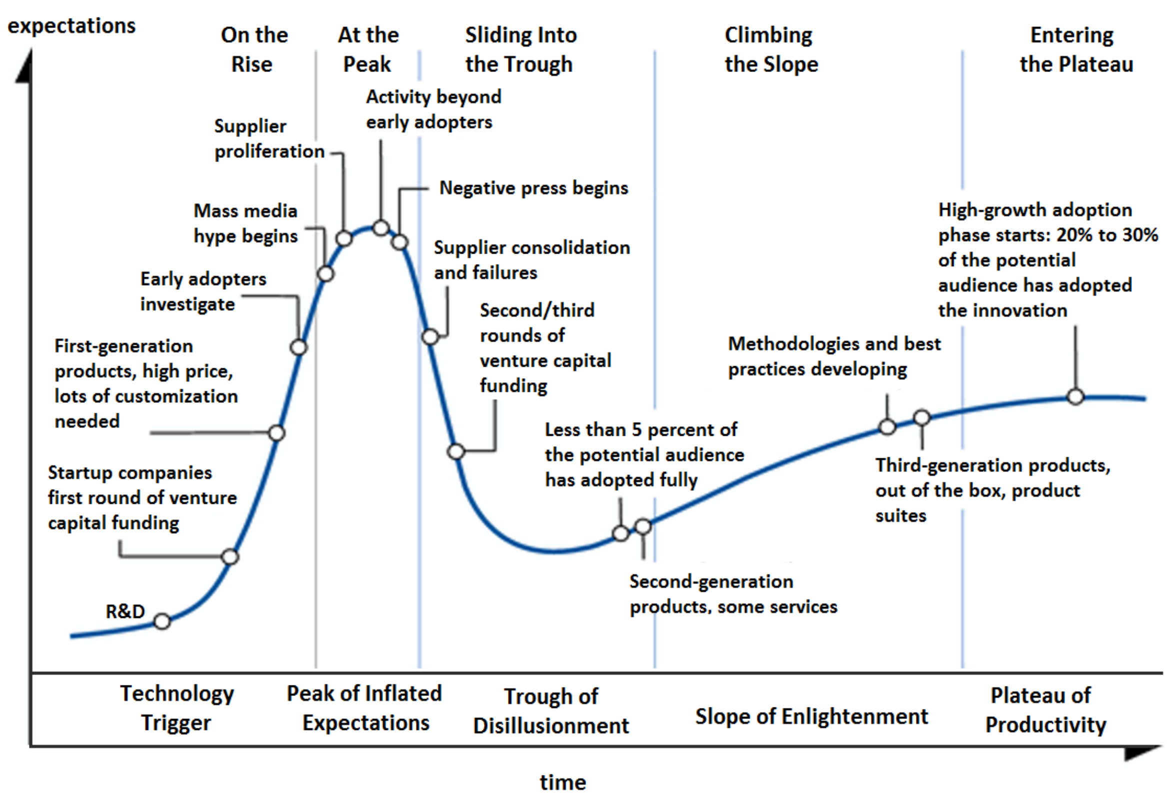

Figure 2 The Gartner Hype Cycle by Olga Tarkovskiy[4]

[3]*The Guardian, 13 May 2023, https://www.theguardian.com/technology/commentisfree/2023/may/13/death-of-mark-zuckerberg-metaverse-meta-facebook-virtual-reality-ai*

[4]*By Olga Tarkovskiy - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=27546041*

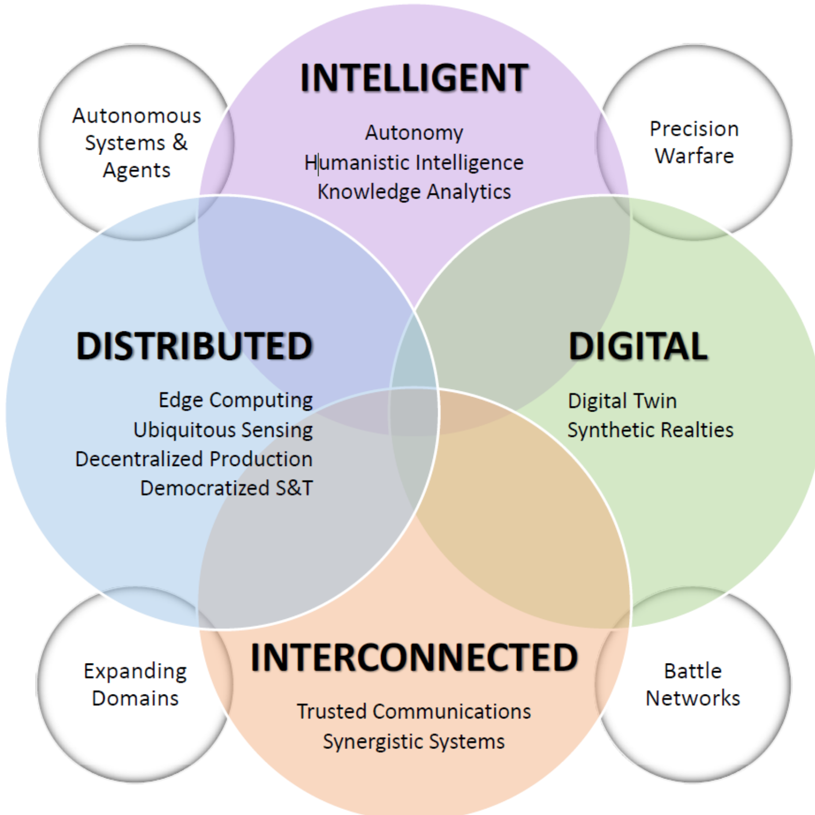

Figure 3 Intelligent-Interconnected-Distributed-Digital with associated military trends (Reading and Eaton, 2020).

can solve problems humans are not capable of. In fact, there is mathematic evidence stating that neural networks can approximate any function; if we have data containing information about a problem, a neural network can find an approach to solve the problem (Strümke, 2023, pp. 73 – 73).

When training a neural network to do something concrete, loss mechanisms are programmed to define what results are given certain scores before it is given access to the dataset. The programmer of the neural network does not control exactly what the neural network emphasizes when working, and the network will point out what it defines as the key findings in the dataset. The consequences of this opaqueness in the algorithms are first that the program can find correlations that humans are not capable of, and second that the correlations they find can be based on completely wrong assumptions (Strümke, 2023, pp. 133 - 134). The need to penetrate the neural network processes and thereby understand what machine learning models have understood about humans is becoming acute at this stage as the cyber warfare domain expands. The entire field is such a complicated and subtle area of research that it is hard for decision makers to understand why and how acute this is (Strümke, 2023, p. 135).

Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) is a term describing the machine's ability to emulate humans in different ways, like holding a conversation.

Machine Learning is the technology underpinning AI and enabling pattern recognition and system self-improvement by use of existing and amassed data.

- Columbia University, 2023.

https://ai.engineering.columbia.edu/ai-vs-machine-learning/

Creating a distributed metaverse training and education framework for Air Command and Control (C2) requires the secure adaptation of these technologies, interconnected, with a wealth of data available for intelligent systems to curate training on individual and group levels. Additionally, and as challenging, it requires a mental shift in educational and pedagogical practices. After such considerations have been met, the distributed metaverse can facilitate training on all levels, at the same time.

The American company Red 6 has already developed and tested augmented reality (AR) software for dogfighting against virtual opponents in extreme conditions, where the threat can be controlled either by an individual remotely, or by an AI (Fink, 2022). With a similar vision for the operational level, NATO Communication and Information Agency is developing and testing a Virtual Joint Operation Centre (JOC) together with industry partners. The vision of a military metaverse where all domains are connected in a multi-domain battlespace, where simulator-driven aircraft are training together with, or opposing, real aircraft with AR representations superimposed in their field of view, and everything connected in real-time to a 3D-representation of the situation in a Virtual JOC, would make the metaverse a “train as you fight” reality.

To paint a picture of the possibilities the metaverse offers in this context, we can envision the following. Given the high level of integration required to create the metaverse, the software itself, through AI, could provide White Team Exercise Control (EXCON) functionality throughout the exercise. The metaverse would then replace the simulator as the “reality” in the wargame, conflating the situational truths from both existing simulator systems and C2 systems, as well as new information gathered from photogrammetry (a 3D-model created from many photos of an area or object) or third-party map systems. Rather than discouraging information gathering from outside sources during training, the metaverse would adjudicate the wargame based on the total of available information, increasing the realism of the exercise. With a 3D representation of the components of a situation (e.g. 3D map, 3D objects of assets and NATO Joint Military Symbology), an entire Air Tasking Cycle can be trained in the metaverse, as a single division against virtual divisions for communication training within a Blue Team, or as separate teams against a virtual Red Team.

This makes the metaverse an interesting tool for training and education, as well as a hub for after-action reviews and recommendations for further training. The system, with the right input, can facilitate simulations of COAs to foster learning, with all participants dispersed. As becomes evident, the use cases described are not limited to Air commanders and staff, even if this paper limits itself to that example for the sake of brevity.

LEARNING AND SKILL DEVELOPMENT IN THE METAVERSE

This section will discuss how learning and skill development can occur in the virtual environments of the metaverse. The discussion is organized into three parts, the first looking at force-level application of the metaverse, the second looking at command and control application with wargaming, and the third looking at how the metaverse can fit into, and possibly enhance, established pedagogical strategies in an educational setting.

When choosing an AI-powered metaverse approach to force-level simulations, the adage "train as you fight, fight as you train" becomes more realistic than ever. With AR software for dogfighting against virtual opponents in extreme conditions, simulator integration, and a virtual gathering of distributed trainees, the training can simulate multi-domain operations completely distributed.

Already in the planning process, the metaverse can supply a feed of different enemy COAs, either based on previously attested enemy COAs or strategies created by the AI to encourage certain changes in behaviour, so the team can observe the consequences of their choices.

In an educational setting, the metaverse lends the same flexibility as it does to wargames, but adds strategies like nano-, experiential-, and game-based learning. For learning to occur, motivation is key, and gamification as an educational medium in the metaverse can increase students' skills, levels of awareness and most importantly, their motivation to learn (Felicia, 2011).

Figure 4 "Wargaming" as seen by Bing AI image creator.

FORCE-LEVEL APPLICATION: THE METAVERSE SIMULATION

The early science fiction vision of the metaverse touches upon an aspect of the technology that cannot be ignored in the discussion, namely the ground-level simulation aspect. With a game-based approach to training, students' motivation to learn, their level of awareness during training, and their skill level can all be increased (Felicia, 2011). The chapter Educational application: The Metaverse and Learning Strategies, below, will look closer at gamification and game-based approaches to learning.

Training can be conducted alone, or together in teams of participants in different physical locations by using the metaverse. The metaverse can provide the team with an additional level of abstraction that allows visualization of communication technology elements. For example, transmission frequencies, interference, bandwidth availability, and radio wave propagation can be viewed in 3D both at a 1:1 scale and from a bird's eye view to aid in understanding the situation. Simultaneously, training can be conducted with participants in simulators or in actual aircraft using technology like Red 6's AR-visualization as mentioned above, seamlessly integrating the physical and the virtual to boost training outcomes.

COMMAND AND CONTROL APPLICATION: THE METAVERSE WARGAME, FROM THE AIR PLANNING PROCESS TO CONDUCTING AIR OPERATIONS

In the planning process, the metaverse can be the facilitator and designer of situations, giving the operational level process the added possibility to test different strategies against a virtual Red team and seeing them play out with different enemy responses before table top exercises or wargaming.

In A History of the Third Offset, 2014 – 2018 (2021, p .63) Gentile et al. sees wargames as essential for the success of the American Defence Innovation Initiative because they promote the kind of innovation that is at the heart of the initiative. The Third Offset is the American Defence Department's strategy seeking to outmanoeuvre advantages made by top adversaries primarily through technology (Wikipedia, April 2023). Innovation with the aim of facilitating adoption of new technology require experimentation to evaluate the efficiency and effectiveness of the technology. The UK Ministry of Defence's Wargaming Handbook defines wargames as simulations of military operations, by whatever means, using specific rules, data, methods, and procedures (UK MOD, 2017). Following this definition, they represent a great arena for testing virtual versions of new technology in simulated environments.

In the article Wargaming-Simulation Synthetic Environment SWORDOM (RAS use case) (2022), Brucato & De Mattia distinguish between wargaming and simulations, denoting wargaming as an analytical tool to extract insights and findings from the participants to inform organizational challenges and complex problems, and simulation as the execution of models through time. In wargames, the participants are the main source of collected data that is interpreted and analysed to answer the initial question, while in simulations the outcome of units in contact is adjudicated by the algorithms, and the human decision making rarely is sufficiently represented.

In the metaverse, both perspectives must be present at the same time to fully realize the potential of the technology. If we imagine a data set containing the processes of and outcomes of n

Figure 5 Concept: Wargaming in the metaverse. Illustration by Fynd Reality AS.

Figure 6 "Air Tasking Cycle" as seen by BingAI image creator.

wargames and n real operations, categorized and annotated to the point where a neural network can be trained on it, we would be able to program a software for creating realistic situational training sessions, containing a realistic representation of enemy tactics, behaviours, and reactions during training.

It is not possible to make a simulator that takes everything into account, nor is it relevant in this case. When the first chess machines won over humans playing chess, they won purely on their superior calculation capacity, by calculating all possible outcomes of a move and choosing the one with the highest probability of winning. Then, as neural networks were trained by playing chess with itself, the program started playing with strategies never before attested in human games and started winning not only as a pure calculation machine, but rather as an actual opponent. Applying this approach to wargaming software would make the metaverse able to facilitate multi-domain operations wargaming against a simulated Red team with realistic and unpredictable reactions.

For the metaverse in a wargaming context, NATO doctrine and standard operating procedure could act as virtual trusses and provide structure and context to the training. Looking at Air C2, both the aim and objectives of a wargame, as well as the setting and scenario, can be created by the metaverse or entered by the wargame designer through an AI. Based on previous wargames or other information from operations and training, the metaverse can recommend a design with objectives it deems necessary for the team to gain more experience.

In the Observe phase of the OODA loop (Observe – Orient – Decide – Act), the team members can enter the metaverse to gather information and start planning. Tools like ACT Innovation's Automated Web Analyzer, Raker, and Exploiter (AWARE) can be used to provide enhanced situational awareness within the metaverse (NATO Innovation Podcast, 2022).

When the team presents their recommendations, the Commander Joint Force Air Component (JFAC) can be another player, or the AI, depending on the training objectives. Following this, creating a scheme of manoeuvre and target development concludes the Orient phase of the OODA loop with the production of the Air Operation Directive. As the team progresses to the Decide phase, determining weaponeering and Air allocation and the development of the Air Tasking Order, the metaverse can run a visualized 3D simulation of the last phase of the OODA-loop: Act.

The metaverse can feed the wargame different enemy actions, either based on a previously attested enemy actions or strategies created by the AI to encourage certain changes in behaviour. This approach demands that previous training outcomes and real operation outcomes are gathered in a big data framework and annotated for a neural network to catalogue and structure. Using this data set, the AI can create strategies for learning that look at the trainees' previous training outcomes and pinpoint the elements they need to focus on to become better decision makers. Systems like Area9 Lyceum[5] can be integrated to achieve this effect and support the AI's foundation to augment the impact of learning.

EDUCATIONAL APPLICATION: THE METAVERSE AND LEARNING STRATEGIES

In an educational setting, the metaverse offers the same flexibility as it does to wargaming, but adds strategies like nano-, experiential-, and game-based learning. This section will outline some of the most relevant possibilities for the metaverse in a pedagogical context.

According to Bandura's theory of social learning, the individual must be motivated to learn for actual learning to occur (Bandura, 1971). The Norwegian Armed Forces Governing Principals of Pedagogy similarly underlines that the learner must be challenged to use their own experiences, conduct critical interpretations, and cooperate with others (Isaksen, 2021). The principle of motivation applies regardless of the form the education takes and is of particular interest in the context of newer generations who are raised to expect a lot more from education than passive listening (Raz-Fridman and Kanterman, 2022).

Commander Geir B. Isaksen, Head of Faculty administration and ADL (Advanced Distributed Learning) at the Norwegian Defence University College, has published a series of papers on the pedagogical shift from traditional lecture-based and fact-memorizing teaching to blended learning strategies in the military context. In the pilot study Twisting the pedagogy in Military Education, Isaksen advocates for a more efficient type of education, harmonizing with the civilian system (Isaksen et al., 2021).

In his suggested approach for their Military Leadership Course, students spend a larger portion of their time on discussion exercises in groups, rather than passive in lectures. The method presented by Isaksen, Problem-Based Learning (PBL), intends to augment the students' analytical abilities and problem-solving skills, using collaboration in groups and critical thinking. The end goal being to produce graduates with a higher understanding and application of mission command, planning and conducting of military operations, and inculcate a bias for action without waiting to be told what to do (Isaksen et al., 2021).

In the context of the metaverse, the method links well with a game-based approach to learning and the gamification of the learning process. Notwithstanding the prevailing view of the last four decades that video games are a waste of time and money, or even dangerous to developing young minds, as an educational medium they can absolutely increase student's skills, level of awareness and most importantly, their motivation to learn (Felicia, 2011).

Procedure training using Virtual or Extended Reality is an example where a gamified approach is both proven effective and economical (PWC,

[5] *https://area9lyceum.com/*

2022). Both the Alliance and the nations are well versed in using heavy and advanced flight simulators as a part of their pilot training, some already using VR headsets like Varjo[6] as part of the simulator. However, simpler, procedure-focused, mechanical training with inexpensive hardware is still not adapted to the degree one would expect when calculating the expenses saved in trainer and trainee travel, decreased equipment attrition, and increased course content retention.

Following an implementation of procedure training in the metaverse, the next phase would be to integrate training for Air C2 Staff. As the training objectives for this group also contains procedure drills, the metaverse can cater to them in much the same way as it can procedure training for equipment. The collaborative and social aspects of the metaverse inherently allow for teamwork drills in failure-safe environments. Tests can be done after rounds of knowledge acquisition and skill development drills, alone or in smaller units.

In this the contours of the future of learning can be seen. Traditional teaching in a classroom setting is already being limited at the Allied nations' military academies. Personnel cost and travel expenses are being cut, while at the same time quality requirements in education is increasing (Isaksen, 2017).

Both as a result of cuts in education sector budgets, and the early availability of technology, the next generations entering military academies will have different expectations for the technology they meet. Children today are making their own games using technology like Roblox[7], and they expect interactivity in their educational content, and to be able to customize and personalize said content. An interesting element that Lebaredian and Raz-Fridman discuss in the podcast Into the Metaverse is that children today seem to be willing to trade visual fidelity for two things: to be with their friends, and to be able to do something for themselves (Raz-Fridman, 2022). According to Lebaredian, the social aspect and the creator aspect is driving the new generations, which in time could impact the way C2 systems are designed and used, especially when interconnected in the metaverse and available through virtual reality and augmented reality.

Building on this, the following vision for the future metaverse learning and training system emerges: the educator can open a training customization interface. Within it they can choose from several templates for the training. Based on the trainees' previous training, experiences from previous real operations, and wargaming exercises, the system presents the most relevant scenario for the trainees in question. The template opens, allowing the educator to either proceed directly to execution of training, or to edit the scenario to fit other training objectives.

The trainees enter the metaverse, where they have access to the tools they need to fulfil the training objectives. The metaverse will guide the trainees and answer their questions using conversational AI in real-time.

In the event that the trainees benefit from adversarial training, the educator can define the capabilities of a virtual Red team during their training. All training activities must be logged to a connected Learning Management Systems (LMS) and gathered for future development of skills for the trainees and for the training system itself through machine learning algorithms, a process called adaptive learning. Using this approach, students' performance is evaluated in real-time, and adjusted to ensure an appropriate learning path (Alexander, 2021). Adaptive learning is already prevalent in language teaching applications like Duolingo[8].

However, though this approach is exciting, a more realistic approach to using the metaverse for learning and training is to acknowledge that different levels of integration will serve different purposes. At one end of the scale is an almost complete simulator where all trainees put on headsets and train exactly as they would in a physical situation, where the metaverse provides everything from three-dimensional environments to virtual pen and paper and connects users in flight simulators with users, or AI, in an Air C2 centre giving orders. At the other end are disparate fragments of the metaverse permeating the training at logical intervals.

As the metaverse is not one software, but rather a convergence of technologies and available hardware, there are several ways in which it can impact training, improve learning and training, and advance staff skills for Air C2 planning, execution, and operational assessment. The first and lowest hanging fruit that the metaverse offers is

[6]https://varjo.com/
[7]https://www.roblox.com/
[8]https://www.duolingo.com/

Figure 7 Gamification of training. Illustration by Fynd Reality AS

distribution. Decentralized and persistent, it allows for joint training sessions without travel, and encourages disaggregation of people and assets.

The complete simulator approach demands that the metaverse must integrate with existing systems and data to ensure the high level of detail and accuracy needed to recreate training scenarios as close to reality as possible. From existing simulators, the system can access algorithms for calculations of lines of sight, availability of fuel and ammunition, or other logistical expenditures. This approach would rely on scripted behaviour to adjudicate the outcome of the training scenario, as described by Brucato and De Marria (2022). With advances in computing power, machine learning trained on existing data and AI presenting the right data to the users, this approach does resemble the science fiction vision of the metaverse and could be possible within the next 20 years (Reading and Eaton, 2020), but probably not sooner.

The more realistic approach offers a vision in keeping with the spirit of both the definition of the metaverse but also training as it is done today. The metaverse would be added to the training in a more fragmented way, and the system would be based on the existing bedrock of integrated technologies but would not be as invasive for the users as a full VR-simulator. This would constitute a more realistic approach to integration of other emerging and disruptive technologies, as the security elements are developed and tested in tandem.

On a C2 level, the existing Air C2 systems must be present and accessible to the trainees in much the same way as they are in operational settings. This will impact the training choices regarding hardware (for example, should the trainees all wear VR-glasses, or can they use mobile phones and PCs at logical intervals). It will also impact the level of immersion the different training scenarios require. Adopting new technology in high-risk fields (such as military, surgery, disaster prevention, etc.) without experiencing breaking integration issues rests largely on whether the technology is being employed appropriately, i.e. where it gives a measurable positive outcome rather than is used as a gimmick. Training with new tech in fields where application of the tech is years away in real situations might just ensure that the tech is never adopted, as it would run the risk of being considered a hype.

If a trainee's main work happens sitting down while using two dimensional screens, they do not automatically gain anything from training fully immersed in virtual reality unless there is a strategic goal for the organization to change the 2D systems to immersive 3D experiences in tactical settings as well. For C2, however, the inclusion of 3D map systems with Blue force tracking and curated military, civilian and open sources information in the same environment could be a way to enhance situational awareness.

As important as security in the research and development of these systems is the user experience and prioritization of human-centric over system-centric approaches. If communication with a machine is to be perceived as comfortable, it must feel useful, and we must get a feeling that the machine understands us (Strümke, 2023, p. 50.). A training system like this should encourage human decision making with the support of system recommendations, so as not to invite vulnerabilities to source manipulation and adversarial machine learning attacks. A well-designed metaverse training system should be able to curate a training scenario based on the trainees' skill levels, the availability of participants in the training, and the success of previous training scenarios.

METAVERSE CYBER SECURITY THREATS AND RISK MITIGATION

This section will discuss some of the security threats that Emerging and Disruptive Technologies (EDTs) faces and how such threats can be met and mitigated when considering the metaverse for NATO Air commanders and staff.

With all new technology, security concerns rise with development and early adoption. The next logical question is of course how such use can be implemented securely. Due to the nature of the metaverse as a convergence of several interconnected systems with distribution as one of its main advantages, secure connectivity and resilience to adversarial attacks and perturbation of data will be key. The above-mentioned applications of the metaverse require integration into already established systems and protocols, where stringent security measures are already in place. The next security concern for the integrated metaverse would then be source integrity and confidentiality, as the metaverse is reliant on cloud storage and is susceptible to source manipulation. As the NATO operational environment expands to include space, cyber, and the broader information sphere, the need to think, plan and operate in a widely dispersed, interconnected, and multi-domain manner will become even more critical (Reading and Eaton, 2020). With such a demand for trusted communications, we can assume that emerging technologies will be developed to the point where they can cater to a growing number of multi-domain sensors for multi-domain missions. Distributed ledger technologies (e.g., blockchain), quantum key distribution (QKD), post-quantum cryptography and AI cyber-agents are examples of emerging technologies that can be used to ensure trusted interactions and information exchange (Reading and Eaton, 2020).

The rising processing capabilities increasingly embedded at the edges of the networks will present new demands for dominance, protection, countermeasures, counter-countermeasures, and other secondary functions. The increasing exploitation of new domains will inevitably lead to the search for domain superiority, with attendant costs and capability demands (Reading and Eaton, 2020).

Taking this into account, it is prudent to think of the metaverse as two connected entities, one for education and training and one for operational support. For an operational integration, it will not be possible to simply separate the metaverse from other networks, as the data flow to and from Air C2 systems, simulators, multi-domain sensors, and user equipment will need to be maintained and secured. The security measures for this metaverse must meet Operations Security (OPSEC) standards. In a training and education context, however, the metaverse can be integrated into existing Air C2 systems and given access only to the information flow needed to support training, ensuring its protection within already established cyber-security measures and data protection through limitation of access.

In the operational setting, the technologies underpinning the metaverse are already being developed and integrated into established architecture. Therefore, in developing future capabilities, rather than thinking of the metaverse as an available software package within the Air C2 systems network, the metaverse should be thought of as a part of the network architecture as it connects data from all available sources, closed and open, to give situational awareness enhancement and operational support.

This requires secure and ubiquitous connection with computing as close to the users as possible to promote disaggregation in an operational setting. The war in Ukraine has given us some insight into the maturity of technology like Starlink[9], launched by SpaceX in 2019. It is a private-sector run, low-earth orbit satellite constellation that claims to provide high-speed, low-latency broadband internet across the globe (Jayanti, 2023). Mykhailo Fedorov, Ukraine's Minister of Digital Transformation, claims that over 150,000 Ukrainians were using Starlink on a daily basis by May 2022 (Jayanti, 2023). That is not to say that the Alliance should be beholden to a single commercial company for such critical communication infrastructure during a conflict, but rather that the existence and successful deployment of such a system should be considered a testament to the viability of the metaverse vision.

During his keynote to the 41st TIDE Sprint in Lillehammer, 2023, Microsoft Norway's National Security Officer, Ole Tom Seierstad, identified what he called "legacy mindset" as the greatest threat to cybersecurity today (Seierstad, 2023).

In the book Tools and Weapons: The Promise and the Peril of the Digital Age (2019), author Brad Smith has a good example of how damaging legacy mindset can be. The WannaCry hacker attack in 2015 was exploiting a vulnerability in Windows XP. Patching it had not been a priority for Microsoft since the entire operating system was deemed obsolete and they wanted customers to move on to the next operating system. The attack was successful because the governmental institutions, including hospitals, had not wanted to invest in the easiest security measure, as it required changes in established procedure (Smith, 2019).

The point that was urgent at that time is now fast approaching critical, as the speed of malware development and vulnerability exploitation is increasing exponentially. If a system is not in the cloud, it cannot be fed security updates at the speed needed to keep up with malware development and must be kept forever offline to ensure the safety of the data (Seierstad, 2023).

As commercial cloud services become available for military customers, third party vendors offer security measures appropriate for military use, and these services are becoming more prevalent as the cost is decreasing and availability increasing. However, as the market represented by the military is relatively small compared to the commercial markets, and the security requirements more stringent, this might present a challenge in the near future. Incentives from the political leadership of the nations to urge commercial actors to support military cloud services might be an option to ensure both financial support and availability for the Alliance demands.

To ascertain a situation picture, correct information is key. The possibility that some of the sources of information have been manipulated or perturbed is both likely and potentially devastating to an operation. Software that aims at improving operational environment understanding and decision making must constantly consider the threat of source manipulation. In the NATO Innovation Podcast (Allied Command Transformation, 2022), Marcus Gaul, Section Head for Analytics and Data Science at ACT, points to the importance of aggregating more than one source of information for the same datatype. If a situational awareness enhancement software gathers data from different sources, including open sources, to create recommendations to the team, it would make it exponentially harder to achieve manipulation as the manipulated sources would clearly stand out and could be excluded by advanced analytics software before reaching the decision makers (Allied Command Transformation, 2022).

Another element of source sensitivity is unintentional manipulation, where the information itself contains components that result in recommendations running counter to NATO values. An example of this could be the result of neural network loss mechanisms making correlations based on wrong assumptions from the data and making recommendations based on these assumptions.

With implementation of automation and AI, security systems require new approaches to protection. A problematic feature of machine learning is the models' vulnerability to source and model manipulation. Generative Adversarial Networks (GAN) are used today to teach image generation models to create images indistinguishable from real images. This is done by setting machine learning models to compete to create better and better images, one model creating images and one looking for clues that it is fake. As a direct result, deepfake images and videos will likely not

[9] https://www.starlink.com/

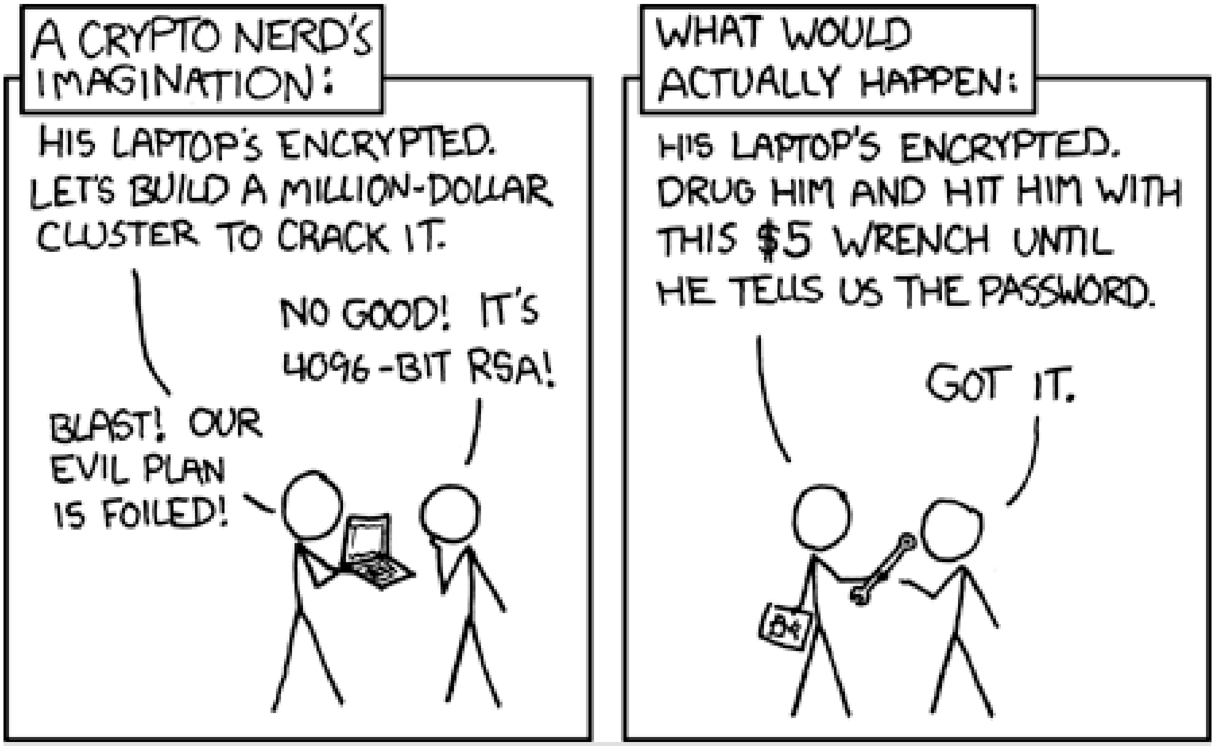

Figure 8 "Security" (xkcd.com, 2023)

be something we can easily disprove in the future (Strümke, 2023, pp. 172 – 173), with the ensuing rise of information warfare.

Machine learning models are also vulnerable to adversarial manipulation of their input, intended to cause incorrect classifications. Additionally, adversarial example transferability happens when an adversarial example designed for one model is also misclassified by another model, allowing someone to perform a misclassification attack on a machine learning system without access to the underlying model (Kurakin et al., 2017).

A remaining point that must be addressed when discussing a wide integration of the metaverse are the ethical discussions that will become necessary with the development of AI. The philosopher Martin Heidegger states that technology is not just devices, but rather the way we understand and relate to the world. Technological development shines a bright light on the values we build society on, without us being completely aware of it. AI, therefore, with its difficult dilemmas, forces us to focus on ethics. (Strümke, 2023, p. 193). The development of the underpinning algorithms for machine learning, as well as the general development of neural networks, require choices to be programmed by humans.

The most prominent example is the programming of semi-autonomous vehicles. The algorithm controlling the vehicles must contain decisions on whom to choose to save (and whom to potentially kill) in the event of an unavoidable accident: the driver and passengers, or the pedestrian(s). Even if farfetched and seemingly theoretical, the situation must nonetheless be a part of the algorithms designed by a human. If different companies rely on the prevailing ethical frameworks of their countries of origin, the result will be that different brands of cars react differently in crisis situations. How long will a brand survive in a traditionally western country if the driver knows that the car will choose to save the pedestrians? Similarly, how long will a brand survive if pedestrians are aware that the brand will choose to save the driver? And how can politicians decide which should have precedence?

These examples are of course extraneous for military AI adoption, but it is a point of contention that the Alliance is bound by a certain understanding of ethics that is not necessarily shared by their competitors in a multipolar world. As the Science and Technology Trends 2020 – 2040 Report reminds us, "A RED weapon system, unrestricted by the physical limitations of the human body, whose behaviour is often unpredictable and inexplicable, would potentially constitute a formidable adversary.” (Reading and Eaton, 2020).

There are already initiatives looking at the ethical application and use of AI to prepare for such eventualities. NATO has launched the Data and Artificial Intelligence Review Board (DARB) with the following aim: “ensuring that the AI applications (Allies and NATO) develop and consider for deployment will be in accordance with six Principles of Responsible Use (PRUs): lawfulness; responsibility and accountability; explainability and traceability; reliability; governability; and bias mitigation.” (NATO, 2023).

On a more pragmatic note, when developing COAs and recommendations in operational settings, there will undoubtedly be situations where, when focusing on minimizing fratricide or judging risk to non-combatant lives, rapid decision-making cycles according to jus in bello will require inclusion of lawyers versed in AI. The EU is currently developing the world’s first comprehensive AI law, regulating the development of AI system and the use of such technology (European Parliament, 2023). In the distributed metaverse, legal aid can be secured from whichever part of the world fits the time zone best, requiring only a connection to the internet.

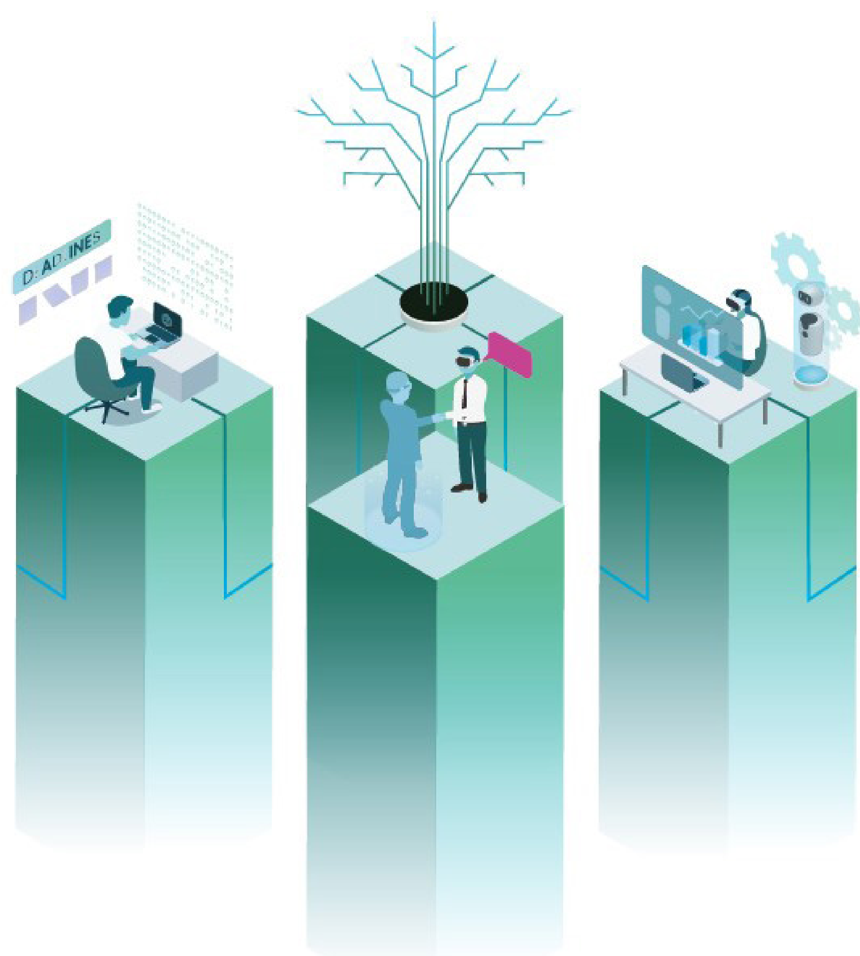

Figure 9 Distributed Collaboration. Illustration by Fynd Reality AS.

SUMMARY

As the discussion above shows, there are a number of use cases for the metaverse that are both relevant and attainable for a global audience and NATO as a whole. For the sake of brevity and clarity, however, the following recommendations focus on how the metaverse can be implemented to increase the skill of Air commanders and staff.

RECOMMENDATIONS FOR NATO

NATO's commitment to increase the Alliance's operational ability in rapidly evolving operational environments will be challenged by the political leadership and the nations' civilian communities to ensure early consideration is given to legal, policy-, economic, and organisational constraints (Reading and Eaton, 2020). Therefore, it is imperative to begin integrating the metaverse in the right areas and with the right vision.

The process of taking new and unchartered technology from the drawing board to full integration into existing systems and cultures is laborious at best. Introducing it through a multi-phased plan will mitigate many of the stumbling blocks by preparing users and decision-makers alike. The key recommendation is therefore to think of any integration in two distinct phases, starting early with the simpler and most clear-cut use cases while preparing for a more holistic integration to maximise the benefits the metaverse offers.

In the short term, the focus should be on establishing acceptance for the simpler and most clear-cut use cases: cost-effective procedure training, making 3D-models of equipment a requirement during procurement, and implementing game-based learning as a pedagogical strategy.

Procedure training using virtual reality, augmented reality, tablets and smartphones, and PCs is already available enough to start integration at a large scale. Connecting these devices and giving access to training and education from any location gives the opportunity to both engage the trainees in a way younger generations will expect (customizable and social) and help with cost reduction through minimizing travel. Another short-term benefit of virtual procedure training is minimized equipment attrition on disassembling and reassembling, going from perhaps hundreds of hours of wear and tear on equipment to just a few hours after virtual training. If 3D models of any new equipment are a part of the procurement requirement, this kind of training can easily be created from existing lesson plans.

As mentioned above, motivation is essential for learning to occur, and future students will demand that the learning environment cater to their expectations for interaction and social components. When employing strategies like game-based learning, the metaverse can, through amassed data, challenge the student to use their own experiences, to conduct critical interpretations, and cooperate with others to solve problems. All in all, these short-term actions can prime the organization to achieve the long-term benefits while both saving resources and motivating younger generations.

In the longer term, NATO should consider the integration of the metaverse through its various components in established architecture (a disaggregated integration approach). The larger vision of interconnected systems, distributed and connected through edge computing and ubiquitous broadband access, will become a reality only when the different technologies are adapted on a smaller scale and time is given to convince both security teams and decision-makers. The technologies underpinning the metaverse are already being developed and integrated into established architecture. So rather than thinking of the metaverse as an available software package within the Air C2 systems network, it should be thought of as a part of the network architecture as it connects data from all available sources, closed and open, to give situational awareness enhancement and operational support.

Following this, the immediate next consideration is to ensure that the data and information is not susceptible to perturbation or unintentional manipulation. To weed out any recommendations made by the system that either run counter to NATO values or are based on wrong assumptions, it is imperative that the allied nations cultivate broad competency in AI, to be able to check recommendations for such unintended perturbations before it is presented to decision makers.

The inclusion of advanced AI, through machine learning methods like neural networks, will also require the cultivation of knowledge and competency in adversarial methods. As this technology is too advantageous to not develop further, competing nations will make sure it becomes a part of the Cyber warfare domain. Simple measures such as gathering information from several sources, rather than one trusted source, should be a fundamental part of development of future systems to avoid information perturbation within the metaverse.

According to the research done by Kurakin et al., injecting adversarial examples into the training set could increase the robustness of neural networks to adversarial examples. The study further claims that adversarial training is the method that provides the most security of any known defence, while losing only a small amount of accuracy (Kurakin et al., 2017). As such, the methods of attack are also the methods of protection when it comes to machine learning. This hypothesis is supported by the article What Artificial Intelligence offers to the Air C2 domain, which concludes that Generative Adversarial Networks will inevitably be a part of the Cyber warfare domain when AI is integrated to a large degree in Air C2 (Koch, 2022).

The next recommendation centres on the use of the metaverse once implemented securely. Koch argues further that AI processes will enable Air commanders to act rapidly and correctly in complex situations, and that this will vastly accelerate OODA-loops at various stages and at machine speed in a collaborative way (Koch, 2022). If so, the increased speed of decision making must be present also in the training scenarios to encourage development of appropriate responses in a changing operational environment. Both Air commanders and Air staff with different division responsibilities could train on their respective responsibilities in an exercise, together against each other or against virtual divisions supported by the metaverse as they play out the OODA-loop.

Building this kind of AI process requires data, and the kind of data that can support such processes must be generated. Rigorous data collection after exercises and thorough after-action reviews should always be fed back into the metaverse to augment the data for future training. Lessons identified should, in addition to human reflections, be extrapolated through the use of machine learning and neural network analysis of everything from verbal communication throughout the active wargame as well as the movement patterns in the 3D maps inside the metaverse. With this approach, connections can be made that can increase both the efficiency and effectiveness of training and wargames.

Finally, with no intention of inviting Artificial Consciousness or events like the Singularity (Wikipedia, 2023) into the discussion, neural networks nevertheless mimic biological thought processes, and display their greatest achievements when thinking more like humans rather than as strong computers. Developing AI with characteristics based on similar frameworks as advanced chess software would make it possible to train against adversaries that act as humans in more unpredictable ways than simulators. Anthropocentric development from the onset could ensure practical and cost-effective application of AI through both training and operational use.

CONCLUSIONS

The metaverse offers a supporting framework for early integration of technology in the field of training and education, especially through wargames and procedure training. To be able to use it as such a framework, acceptance must be cultivated throughout the organization and the use of its underlying technologies must be proven beneficial.

Such acceptance can be achieved by identifying short- and long-term goals for the integration. As with all new technology, it is imperative that both the end-users and stakeholders see the benefits of changing their set ways. Starting with the main goal of using the metaverse to improve Air commander and staff skills, the key take away of this paper is the plan for long-term integrations while simultaneously maximizing the short-term benefits, e.g. using it for virtual reality procedure training, wargaming and game-based learning.

Though the NATO's Data and Artificial Intelligence Review Board and the EU AI Act, among others, will impact how these technologies can and will be used in the horizon of 2024 – 2044, the short-term recommendations identified in this paper as a first priority for using the metaverse to increase Air commanders and staff skills ought to be sufficiently beneficial for consideration alone.

Figure 10 "Wargaming Air operation" as seen by BingAI image creator.

REFERENCES

Alexander, S. (2021). Adaptive Learning: How Technology Is Breaking Down Barriers In Education. Forbes. Accessed on 25.06.2023 at

https://www.forbes.com/sites/forbestechcouncil/2021/05/21/adaptive-learning-how-technology-is-breaking-down-barriers-in-education/?sh=67bc318f126f

Allied Command Transformation (June 2022). Situational Awareness Enhancer: AWARE. NATO Innovation Podcast.

https://www.act.nato.int/newsroom/multimedia/podcasts/

Ball, M. (2022). The Metaverse: And How It Will Revolutionize Everything. Liveright.

Bandura, A. (1971) Social Learning Theory. General Learning Press, New York. Accessed on 08.06.2024 at

https://ia903002.us.archive.org/15/items/BanduraSocialLearningTheory/Bandura_SocialLearningTheory.pdf

Brucato V., De Mattia, S. (2022). Wargaming-Simulation Synthetic Environment SWORDOM (RAS use case). CA2X2 Forum 2022 (Computer Assisted Analysis, Experience, Experimentation). NATO's Digital Transformation Now & Beyond.

Columbia University. (2023). Artificial Intelligence (AI) vs. Machine Learning. The Fu Foundation School of Engineering and Applied Science. Accessed on 13.06.2023 at

https://ai.engineering.columbia.edu/ai-vs-machine-learning/

Deloitte.com. A whole new world? The metaverse and what it could mean for you. (2023). Deloitte. Accessed 04.06.2023 at

https://www2.deloitte.com/us/en/pages/technology/articles/what-does-the-metaverse-mean.html

European Parliament. (2023). EU AI Act: First regulation on artificial intelligence. News European Parliament. Accessed on 26.06.2023 at

https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Faggella, D. (2013 – present). AI in Business. Palantir's Shannon Clark on Overcoming Cultural (and Emotional) Challenges of AI Adoption. Emerj Artificial Intelligence Research.

www.emerj.com

Felicia, P. (2011). Handbook of Research on Improving Learning and Motivation Through Educational Games: Multidisciplinary Approaches. Information Science Reference. USA.

Fink, C. (November 2022). Real planes, virtual adversaries in red 6 ar. Forbes.com. Accessed on 07.11.2023 at

https://www.forbes.com/sites/charliefink/2022/11/07/real-planes-virtual-adversaries-in-red6-combat-simulation/?sh=30df439117b4

Gentile, G., Shurkin, M., Evans, A. T., Grisé, M., Hvizda, M., Jensen, R. (2021). A History of the Third Offset, 2014–2018. RAND Corporation. Santa Monica, CA. Accessed on 07.11.2023 at https://www.rand.org/pubs/research_reports/RRA454-1.html

Goode, Claire. (2019). Best practice principles for Professional Military Education: A literature review. Journal of Defense Resources Management. Vol. 10. Dunedin. New Zealand.

Hackl, C. (2023). Into the Metaverse: The Essential Guide to the Business Opportunities of the Web3 Era. Bloomsbury Business.

Harvey, A., S. (2021). The Levels of War as Levels of Analysis. Military Review. Army University Press. USA.

Humphreys et al. (2021). 2021 Breakthrough of the year. Science. Accessed on 04.06.2023 at

https://www.science.org/content/article/breakthrough-2021

Isaksen, G. (2017). How Video Lectures Can Free Up Time For Other Learning Activities. Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).

Isaksen, G. B. (2021). Twisting the pedagogy in military education experiment. Scandinavian of Military Studies.

https://doi.org/10.31374/BOOK2-K

Jayanti, A. (2023). Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public

Purpose? Belfer Center for Science and International Affairs, Harvard Kennedy School. Harvard Kennedy School. Accessed on 14.06.2023 at

https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose

Johnsen, G. and Bjørge, S. (2023) I luften kan Norden bli en stormakt. Men på bakken finnes en norsk bekymring. Aftenposten.no. Accessed 04.06.2023 at

https://www.aftenposten.no/norge/i/bgWpzd/i-luften-kan-norden-bli-en-stormakt-men-paa-bakken-finnes-en-norsk-bekymring

Joint Staff J7, Deployable Training Division (DTD). September 2019. Joint Headquarters Organization, Staff Integration, and Battle Rhythm. Insights and Best Practices Focus Paper. Third Edition. USA.

Knight, W. March 2019. How malevolent machine learning could derail AI. MIT Technology Review, accessed 20.06.2023 at

https://www.technologyreview.com/2019/03/25/1216/emtech-digital-dawn-song-adversarial-machine-learning/

Knight, W. (2022). The US Military Is Building Its Own Metaverse. Wired.com. Accessed 31.05.2023 at https://www.wired.com/story/military-metaverse/

Koch, W., Dr., (2022), What Artificial Intelligence offers to the Air C2 domain?, OPEN Publications Volume 7, Number 5, accessed 31.05.2023 at https://issuu.com/spp_plp/docs/what_artificial_intelligence_offers_to_the_air_c2_?fr=sNzFiMzQ4MjEzNTc

Kurakin, A., et al. (2017). Adversarial machine learning at scale. ICLR.

https://arxiv.org/pdf/1611.01236.pdf

McIntosh, V. (2022). Dialling up the danger: Virtual reality for the simulation of risk. Frontiers. Accessed 22.05.2023 at

https://www.frontiersin.org/articles/10.3389/frvir.2022.909984/full?hss_channel=lcp-12582246

NATO (2023) NATO's Data and Artificial Intelligence Review Board. Accessed on 06.11.2023, at

https://www.nato.int/cps/en/natohq/official_texts_208374.htm

Norges offentlige utredninger 2023. (2023). Forsvarskommisjonen av 2021. Departementenes sikkerhets- og serviceorganisasjon. Teknisk redaksjon. Oslo.

PWC. (2022). What does virtual reality and the metaverse mean for training? Emerging Technology. Accessed 13.06.2023 at https://www.pwc.com/us/en/tech-effect/emerging-tech/virtual-reality-study.html

Raj, B. (2018). A Simple Guide to the Versions of the Inception Network. Toward Data Science. Medium. Accessed on 09.06.20203:

https://towardsdatascience.com/a-simple-guide-to-the-versions-of-the-inception-network-7fc52b863202

Raz-Fridman, Y. & Kanterman M. (2021). Into the Metaverse. Building the Metaverse with Marc Petit of Epic Games. Bloomberg Intelligence.

https://www.intometamedia.com/about

Raz-Fridman, Y. & Kanterman M. (2022). Into the Metaverse. Into the Omniverse with Nvidia's Rev Lebaredian. Bloomberg Intelligence.

https://www.intometamedia.com/about

Reding, D. F., and Eaton, J. (2020). Science and Technology Trends 2020 – 2040, Exploring the S&T Edge. NATO Science and Technology Organisation. Brussels.

Reding, D. F., De Lucia, A., Blanco, A. M., Regan, L (Col), Bayliss, D. (2023). Science & Technology

Trends 2023-2043. Across the Physical, Biological, and Information Domains. NATO Science and Technology Organisation. Brussels.

Saunders, R., and Souva, M. (2020). Air superiority and battlefield victory. Research & Politics, 7(4). https://doi.org/10.1177/2053168020972816

Smart, J. et al. (2007). Pathways to the 3D Web. A Cross-Industry Public Foresight Project. Metaverse Roadmap. Accessed 04.06.2023 at

https://www.metaverseroadmap.accelerating.org/

Smith, B., Browne, C., A. (2019) Tools and Weapons: The Promise and the Peril of the Digital Age. Penguin Press. USA.

Song, D. (2019). Privacy-Preserving Smart Contracts at Scale. EmTech MIT Technology Review. Accessed 31.05.2023 at

https://www.youtube.com/watch?v=IDdD7cvVQiM

Strand, G., et al. (2022). Forsvarssektorens evne til å ta i bruk ny teknologi. Forsvarets Høgskole. Norway.

United Kingdom Ministry of Defence. (2017). Wargaming Handbook. Shrivenham. United Kingdom.

Wikipedia. (June, 2023). Technological singularity. Accessed on 22.06.2023 at

https://en.wikipedia.org/wiki/Technological_singularity

Wikipedia. (October, 2023). Garther hype cycle. Accessed on 04.10.2023 at

https://en.wikipedia.org/wiki/Gartner_hype_cycle

Wiktionary.org. (2023). μετά. Accessed on 13.06.2023 at https://en.wiktionary.org/wiki/%CE%BC%CE%B5%CF%84%CE%AC#Ancient_Greek

xkcd.com. (November 2023) Security. xkcd – A webcomic of romance, sarcasm, math, and language. Accessed on 07.11.2023 at

https://xkcd.com/538/

Metaverse: A Tool for Improving Air Commander
and Staff Skills

www.openpublications.org