Unlocking the Military Potential of the Metaverse

Rob Solly
10 Bishops Square
London, E1 6EG
UNITED KINGDOM

robsolly@improbable.io

Jennifer McArdle
4100 Fairfax Dr. Suite 500
Arlington, VA 22203
UNITED STATES

Jennifer@improbable.us

ABSTRACT

The metaverse, or a metaverse, is the latest buzzword to capture the imagination of the defence community, eliciting excitement, ridicule, and confusion in almost equal measure. While there's no formal definition, there's an increasingly common understanding among technologists in sectors ranging from sport and entertainment to fashion and engineering: a metaverse is "a series of interconnected persistent, and immersive virtual worlds that afford their users a sense of agency or presence". This is happening right now. Investments are pouring into companies that are already building the technologies that will support the metaverse. It promises to revolutionise both civilian life and government, especially national security and defence. Drawing on the technologies pioneered by Improbable for commercial metaverse applications, our defence business is exploring the application of those tools to military modelling and simulation (M&S). This paper explores the various ways in which metaverse technologies could affect traditional military M&S tools across a range of application areas, from capability development and procurement, to training and education, mission rehearsal and others. It also draws on targeted interviews with defence professionals to demonstrate how these technologies have the potential to transform military readiness and cohesion within NATO.

1.0 INTRODUCTION

In 1995 Bill Gates sat down with David Letterman and attempted to describe an emerging phenomenon, something Letterman called "this internet thing." The Internet, as Bill Gates described it, was a "place where people can publish information" or "send electronic information." Letterman mentioned that he heard people could watch a baseball game on the Internet, but he remained unconvinced by its utility, asking "does radio ring a bell?" When Gates stated that unlike radio an individual could listen to a game at their leisure, at the time of their choosing, Letterman quipped, "[do] tape recorders ring a bell?" Gates attempted to convince Letterman that society was on the cusp of something truly transformative, but his description remained wanting. Letterman's final verdict was that this "thing" would fall flat, or as he stated, "It's too bad there is no money in [computers and the internet]" [1].

Gates's struggle to explain the internet is not dissimilar to the struggles of today's many proponents of the metaverse. At the time, the internet seemed nebulous and ill-defined. It seemed duplicative. There is a general belief in the commercial sector that we find ourselves at a similar inflexion point: the metaverse today is the internet of 1995 and, like the internet, the economic potential of a metaverse-driven future is estimated to be immense. Indeed, recent studies have estimated that metaverse technologies are poised to contribute 2.8% to global GDP within the next decade, or $3.01 trillion [2]. To bring that virtual future into existence, commercial industry investments in the technologies that will support any future metaverse have skyrocketed, with sectors as diverse as entertainment, retail, manufacturing, tourism, real estate, education, and medicine seeing real value in its future adoption [3]. The defence establishment has likewise taken notice. The UK Ministry of Defence is supporting research into the metaverse, while the US Air Force has filed a trademark application for their future SpaceVerse [4] [5]. NATO, likewise, has started to dip its toes into this virtual future, through sponsored research and conferences [6]. The metaverse—whether in the commercial sector or defence—has become the *buzzword du jour* eliciting excitement, ridicule, and confusion in almost equal measure.

1.1 What is the Metaverse?

Despite its ubiquitous presence across popular culture, the media, and the commercial and defence industries, the term "metaverse" still generates an understandable amount of bewilderment. No true definition exists. However, the commercial industry has broadly started to coalesce around a common definition—or the key attributes—of the metaverse. In short, if one were to provide a workable definition, it would be the following: the metaverse is a series of interconnected, persistent, and immersive virtual worlds that afford their users a sense of agency and presence [7] [8].

Part of the opacity surrounding the term can be tied to how a metaverse is used colloquially— "a metaverse" is often used interchangeably with "the metaverse." In reality, these are two different things. A metaverse is a single virtual world. Theoretically, any corporation or group of programmers can create their own metaverse, much like how any individual or entity can create their own network. At present, this is how most metaverses seem to be emerging—a series of single virtual worlds where corporations maintain the servers, dictate user conduct, and determine the ways in which the space can be employed. The metaverse, however, is a series of interconnected virtual worlds based around a shared open architecture that appear as one continuous world to users. Much like how the world wide web allows a range of resources to be accessed via a common protocol, the metaverse will likewise allow different entities and servers to interconnect via a shared set of agreed upon standards and interfaces [9]. While in the near term various metaverses—such as a Meta metaverse, a Roblox metaverse, or metaverses supported by these authors' company—that act as separate "walled gardens," are emerging, the aspiration among commercial companies to achieve "the metaverse" is strong. Economic forces will create incentives for interoperability among metaverses, as a strong desire exists for content —like digitally acquired goods, such as avatars, to be metaverse agnostic. As a result, opportunities exist for the defence modelling and simulation (M&S) community to draw on advances made in commercial sectors.

Drawing on our commercial parent company's experience shepherding various technical facets of metaverses into existence, our defence business's application of those tools to military M&S, and targeted interviews with defence professionals, this paper proceeds in three parts. It first maps the technology stack that is often associated with a metaverse and outlines how various facets of that technology stack may be able to augment—or at the very least, provide new avenues of exploration for—defence M&S. It then employs NATO's *Modelling and Simulation Masterplan* as a rubric to explore the application of these metaverse technologies to the traditional application areas of defence M&S: capability development, procurement, training and education, support to operations and mission rehearsal. It shows that the technologies that will empower a metaverse may require an expansion beyond the traditional application areas of defence M&S. Indeed, metaverse-based tools have the power to inject M&S more deeply into rapid adaptation, in service support, autonomy, and personnel management practices. What's more, they could also facilitate deeper interoperability across these application areas, transforming military readiness and cohesion within NATO member states and across the broader alliance.

2.0 MAPPING THE TECH STACK BEHIND THE METAVERSE TO M&S

To trace where metaverse technologies may augment, or even supersede, traditional defence M&S tools, one first needs to deconstruct at a high-level the technology stack behind concepts of a metaverse. While a metaverse can be broken down into a variety of different layers, for the purpose of this paper, a metaverse generally is composed of seven different layers: the user interface, cyber-physical interface, runtime infrastructure, fed by a content ecosystem, running on compute, and enabled via networking and blockchain / distributed ledger technologies, as shown in Figure 2-1 below.

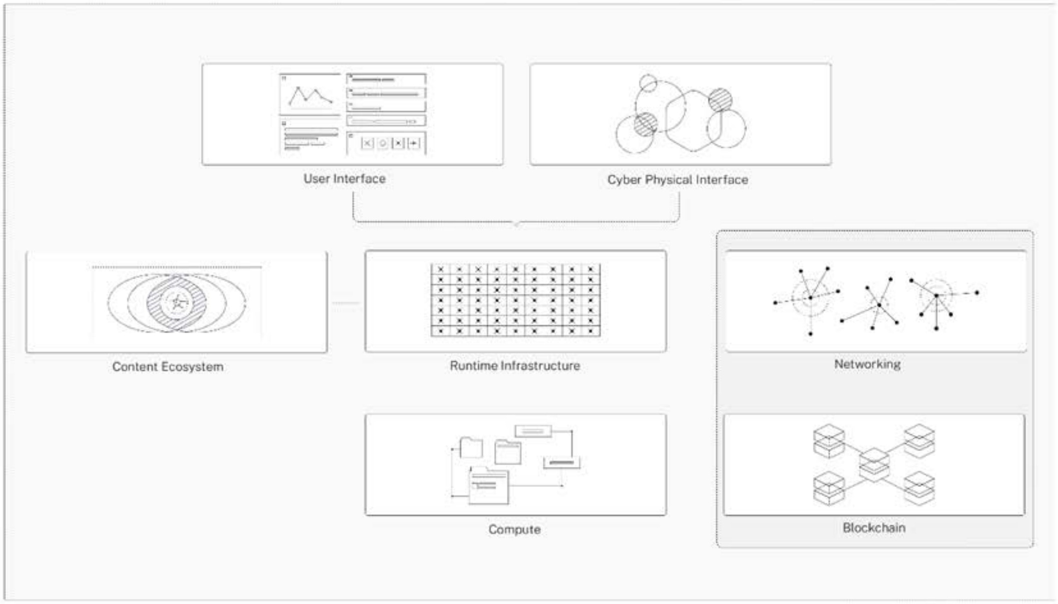

Figure 2-1: The Metaverse Tech Stack

2.1 The User Interface

Much like how warfighters and training providers need a means to “enter” a simulation, users—whether military or commercial—will also require one or more mechanisms to partake in a metaverse. Access to a metaverse can occur through a range of user interfaces, depending on individual preferences. Extended reality tools, like virtual reality or augmented reality, are often highlighted as the types of user interfaces that will facilitate more immersive and meaningful experiences. However, despite popular portrayals of the metaverse as an extended reality experience, access to a metaverse is not dependent on these devices. Users may choose to visually access a metaverse via their laptop, tablet, or even a mobile phone. As defence begins to conceptualise “military metaverses,” the tools that are traditionally used for synthetic training—whether new or legacy—will also be employed to ensure user access to these future worlds. Like the civilian sector, many of these interfaces will be virtual reality or augmented reality headsets, laptops, or mobile phones, but the military may also work to integrate full-motion simulators and operational systems, like command-and-control systems, that can be employed for training or operations.

Visual interfaces, on their own, however, are likely to fall short when facilitating an immersive experience that affords users a sense of “presence.” Commercial companies are exploring the employment of interfaces that are poised to create far more interactive metaverse experiences—beyond the visual domain. Within the modelling and simulation literature, these have traditionally been referred to as mixed reality systems: the use of sensors and other tools to trigger responses across the full range of a user’s senses—to include visuals, haptic feedback, spatial audio, and smell. In a military context, for instance, simulated imagery of a pine forest could act as a catalyst for the injection of pine aroma, while the pull of a trigger during gunnery training could generate a recoil and muzzle flashes. While the military already employs haptics, motion capture technologies, and biometric sensors, commercial research and development may further fuel advancements that the defence M&S community can leverage. Indeed, sensors in the Apple watch are so sensitive that they can detect whether a user is clenching their fist or releasing it. Gamers—arguably the early-adopters of metaverse type experiences—fully expect to adopt haptic gloves or body suits to more fully immerse themselves in virtual experiences like those imagined in *Ready Player One*. Micromechanical systems, a new form of haptic device, release an ultrasonic sound, a form of mechanical energy, that users have described as creating a “force field” in front of them [7]. Test subjects have reported sensing everything from a soft teddy bear to a bowling bowl based on the micromechanical stimulation of the fingertips. Such capabilities may find immediate applications simulating military medical procedures or operations in environmentally hostile conditions like the Arctic.

2.2 Cyber-Physical Interface

More than just human-focused sensory experiences, the metaverse also stands to benefit from the integration of cyber-physical systems, in particular the proliferation of the Internet of Things (IoT). Indeed, just as an interface exists into the metaverse for human participants, a cyber-physical interface will also exist for technology-based systems, such as a military system or platform, or even complex socio-technical systems, like critical infrastructure. Commercial industry has conjectured that the interconnection of cyber-physical systems and the metaverse can best be described as digital twins— digital replicas of physical things and systems [10]. By incorporating digital scans of physical objects, with IoT sensors that capture live data feeds, new economic and industrial opportunities will continue to be unlocked. Furthermore, a cyber physical infrastructure could connect multiple digital twins and the systems they represent into an “Internet of Digital Twins” [11]. For instance, next-generation power infrastructure will rely heavily on real time data that connects weather sensors, solar panels, wind turbines, battery management systems, and grid systems together. A metaverse, replete with a digital twin of renewable energy infrastructure will allow society to better optimise sustainable power usage [12]. In the tourism industry, a metaverse could be updated in real-time to reflect a physical space: a metaverse that simulates New York’s Times Square could be continuously updated as real people and vehicles move throughout the physical location, giving virtual tourists a far richer and realistic experience.

Such thinking isn’t unique to the commercial world. The military has experimented with the use of digital twins since 2010 to help shorten the research and development cycles associated with select weapon systems, such as DARPA’s adaptive vehicle product program. Military requests for proposals are replete with asks for digital twins of systems and platforms. By transferring data from physical systems to the digital environment via sensors, the technology allows developers and acquisition professionals to analyse, model, and test various scenarios prior to subjecting those systems to those same stimuli in the real world [13]. Modern military systems like aircraft contain thousands of sensors that produce terabytes of data per sortie. Digital twins of those same platforms can help manufacturers and users better manage required maintenance, improve fuel consumption, and reduce overall costs. Such interest is only set to increase. As militaries work to adopt complex command and control systems built around distributed systems and kill webs, digital twins of those architectures could help to assess their survivability and resilience in the face of a contested and complex battlespace [14]. Digital twins of socio-technical systems, like those that simulate urban environments, may also allow the military to better grapple with some of the “woollier” elements of warfare, such as human sentiment, cognition, and decision.

The successful implementation, however, of a metaverse that includes digital representations of real-world entities requires that the community grapple with various technical challenges—from data ingestion to data management, and M&S. As the commercial industry seeks to integrate cyber physical systems into the metaverse, it is likely that many lessons learned will prove valuable to the defence M&S community and may warrant emulation.

2.3 Runtime Infrastructure

The runtime infrastructure of a simulation is the middleware—a series of software services that allows for a simulation to be quickly composed and run, while also ensuring interoperability when implementing a distributed simulation. For instance, simulation development tooling helps to ensure that a synthetic environment can be quickly composed to meet a user's experiential or analytic needs, without the six-month to a year lag time typically associated with the development of simulated environments. In military M&S, the runtime infrastructure is a fundamental component of the various interoperability protocols and information exchange models that allow various simulations to work together as a single federation. In a federation, it appears to the simulation users that they are interacting with a single simulation as opposed to many distributed simulations that may be stitched together. Defence M&S relies primarily on three widely used standards to ensure interoperability across distributed simulation architectures, to include Distributed Interactive Simulation (DIS), High Level Architecture (HLA), and the Training Enabling Architecture (TENA) [15]. Architecture-dependent, well-defined interfaces can also be used to maximise the performance of a runtime environment, in lieu of a standard.

Like the defence M&S community, the commercial metaverse community must also stitch disparate simulations together to ensure interoperability. Indeed, interoperability is one of the core organisational and technical challenges that metaverse developers will have to grapple with. Key to most visions of the metaverse today is a belief that users can take data and content—such as an avatar, clothing accessories, or their own personal data—from one virtual world to the next, allowing that data and content to be modified, sold, or exchanged with other goods. This requires that the commercial metaverse community work together to define standards and interfaces that allow these worlds to work together. More than that, however, developers will also need to develop code that can interpret, modify, and approve third-party virtual content for use in one virtual world to the next [7]. Commercial companies like our own are already trying to provide common standards to ensure that creation tools are interoperable by advocating for a common metadata ontology, 2D image and 3D object format, and universal scripting system. More will have to be done, but there is room for optimism. Just as economic incentives drove common commercial adoption towards a standard internet protocol, it is likely that similar economic trends will create an impetus for common standards across the metaverse, or for intelligent software that can interpret between multiple ever-changing standards. New interoperability standards that transcend legacy standards like HLA or DIS may prove beneficial to defence M&S.

2.4 Content Ecosystem

The content that undergirds a metaverse includes all the data and models that make up that virtual world. Much like virtual and constructive environments deployed in a military context, a metaverse will include logical, stochastic, physics, and artificial intelligence models that govern the movement, engagement, and interactions that take place within that virtual space. Similarly to how the military employs terrain models so users can visualise an area of operations, the metaverse will also place users in a rich visualised environment—whether that content mimics the physical world or is far more fantastical, placing users in far-off science-fiction landscapes. Two trends that are driving metaverse content creation are worth noting—and theoretically emulating—within the defence M&S community: the first is the proliferation of non-fungible tokens (NFTs) and the second are metaverse platforms that provide no-code or low-code opportunities for content development.

Most famously – or infamously – these can represent anything from in-game avatars to digital artworks. But they can also represent real-world assets, from real estate deeds to medical records to educational and training data. Digital representations of goods are not a novel concept, yet within a metaverse, NFTs are frequently tied to blockchain or tamper-resistant distributed ledger technologies that create an economic ecosystem around them. In short, in many instances, NFTs can act as a form of digital currency. As a result, strong economic incentives exist for their development [16]. Many physical content creators with built-in fanbases are already taking advantage of NFTs. Brands like Star Wars, Gucci, and the National Basketball Association (NBA) are developing NFTs to tap into the same commercial interests that sell their physical goods, but instead with unique virtual items or digital replicas specifically for use in the metaverse.

Content creation, however, will not be limited to large-scale commercial enterprises, like fashion houses or sports leagues, that can invest in their digital development. New tools are emerging that are democratising content creation. Roblox provides a no-code platform that allows users to develop their own games through an asset store of templates that can be modified based on game goals. Users within the Roblox ecosystem can play the games developed by other users, creating powerful platform network effects. Epic Games' MetaHuman release in Unreal Engine 5 provides developers a unique framework to create their own realistic human characters or avatars in minutes. Other applications, like Open-AI's DALL-E or Automated Insights—are exploring the use of machine learning to streamline unique content generation.

These two trends may have implications for defence M&S. In the first instance, NFTs are creating a marketplace of content that can be bought and sold across metaverses. Such a system could theoretically be applied to defence M&S, helping to create a far richer content-ecosystem, should a greater emphasis be placed on modular, open-system architectures and microservices. Microservice architectures, which form applications as collections of modular services, with their accompanying interface specifications, pave the way for replacing modular parts of a system with more performant, appropriate, or even completely new modules or models [17]. Should microservices be treated as NFTs, incentives may exist for content developers to prioritise microservice-based approaches as economic incentives could be derived from their very interoperability and reusability. Unlike present acquisition paradigms in defence for models and simulations, a marketplace could instead emerge to drive down costs for defence providers, while likewise, creating greater economic benefits for content producers.

Secondly, should low, or preferably no code developer tools emerge within the defence M&S community, a larger community of content producers could emerge—particularly among those that are charged with wargame design or training development. No code development tools would provide flexibility to defence professionals, allowing them to adapt training or decision support tools without having to work through defence bureaucracies' byzantine acquisition processes or through a defence contractor to make software changes. It would also allow virtual wargames or training events to be adapted on the fly based on lessons learned in the field without having to contract with developers to update game injects or simulations.

2.5 Blockchain and Distributed Ledger Technologies

While not a requirement for a metaverse, distributed ledger technologies, to include blockchain, are frequently included in many commercial conceptions of the metaverse technology stack, as they help to enable virtual economic ecosystems, from the purchasing of digital land to the secure transfer of digital goods and trusted user authentication. A distributed ledger is a database or a record of consensus with a cryptographic audit trail that is maintained and validated by various nodes within the network. Distributed ledgers can be decentralised or centralised, depending on the rights of the participants. A blockchain is a means to implement a distributed ledger—it enables real-time access, validation, and record-keeping of transactions, also known as "blocks," within a ledger after certain types of predetermined criteria are met [18]. Ledgers are meant to be immutable—they can't be changed without prior consensus, or agreement, among participants in the network. As a result, blockchains can be used to provide high-quality, trusted, and authenticated data at scale [19].

Unsurprisingly, it is the very security provided via blockchain that provides the rationale for it to underpin cryptocurrencies, like the Bitcoin network. This same security is the reason that distributed ledger technologies are being employed—or planned to be employed—within many metaverses to manage the trusted buying and selling of NFTs. Together NFTs and distributed ledger technologies are meant to compose the economic lifeblood of the metaverse, much like how payment rails, such as SWIFT or VISA, provide the economic foundation for aspects of our present economic ecosystem.

Distributed ledger technology, however, will not solely facilitate a metaverse economy. As Epic Games' founder, Tim Sweeney, has noted, "I've come to the realisation that blockchain is really a general mechanism for running programs, storing data, and verifiably carrying out transactions. It's a superset of everything that exists in computing" [7]. For this reason, the FY2020 U.S. National Defense Authorization Act directed the Under Secretary of Defense for Research and Engineering to brief the U.S. congressional defence committees on the potential uses of distributed ledger technologies for defence purposes [20]. The findings were striking. Indeed, five core areas were highlighted as potential distributed ledger technology applications in defence:

1) Improve cybersecurity: The tamper-evident nature of distributed ledger technologies makes them difficult to compromise. A successful attacker would have to gain control of not one, but many participants' devices. As a result, distributed ledger technologies can be employed within many enterprise applications to ensure cybersecurity, while also helping to facilitate multi-factor and multi-party authentication.

2) Reduce single points of failure in decision-making during catastrophic events: Distributed ledger technologies can mitigate against single points of failure in high-risk decision-making by employing cryptographic proof of identification. Due to its distributed nature, it also has robust properties. Distributed ledger technologies are more likely to maintain operations in catastrophic conditions when compared against other centralised IT systems.

3) Improve efficiency of defence logistics and supply chain operations: Distributed ledger technologies can mitigate against the risks of counterfeit, manipulated, or non-conforming components within the defence supply chain by acting as a trust enabler. These technologies can provide greater visibility into the origination of a component and its destination by acting as a "track and trace" system.

4) Enhance the transparency of procurement auditing: Blockchain can act as a tamper-resistant, tamper-evident, and single source of truth to benchmark against waste, fraud, and abuse within the procurement system. Incorporating distributed ledger technologies into an e-procurement system enables security, while also providing a capability that can be updated and shared in real time amongst stakeholders to promote transparency.

5) Allow innovations to be adapted by the private sector for ancillary use: Distributed ledger technologies can facilitate a stakeholder network that could expand across the defence ecosystem—from a manufacturer, to transportation, suppliers, and defence customers. Having all defence stakeholders together on one distributed ledger provides traceability, while also enabling a governance structure that allows for trusted operations, business processes, compliance, talent management, and technology iteration. [19]

While it is unlikely that defence M&S will implement anything like how blockchain or distributed ledger technologies are employed in commercial economic ecosystems, the use of distributed ledger technologies for trusted bookkeeping, and more broadly, their potential applications across the defence enterprise are reason for considering their use in future defence M&S applications. Indeed, all the applications identified by the U.S. Under Secretary of Defense for Research and Engineering have resonance within defence M&S, from cybersecurity, to supply chain considerations, and more streamlined procurements. As M&S is used more widely to support military operations, drawing on tools that mitigate against single points of failure and ensure trust will be necessary, particularly for complex command and control architectures built around kill webs. Moreover, a distributed ledger could help facilitate a marketplace model for content, enabling the defence M&S community to draw on a greater degree of microservices.

Finally, one other application is worth considering: multi-level security (MLS). MLS is a core requirement for effective training, experimentation, and decision support across NATO. MLS will allow country-specific platforms and systems—for instance the U.S. F-35 joint strike fighter and the French Dassault Rafale—to interconnect across differing levels of classification. At present, developing MLS solutions remains an aspiration for many commercial industry partners and is yet to be effectively integrated into training events, experiments, or decision support tools. Assuming that the necessary amount of compute is available and managed, new methodologies like distributed ledger technologies may provide a path forward for the effective implementation of MLS across the NATO military alliance.

2.6 Networking

Networking technologies allow simulated environments to be distributed to users, regardless of their physical location. In short, these technologies allow for the exchange of data across various computing devices via transmission lines, switches, and routers, among other devices [21]. Drawing on various networking technologies, the defence M&S community has invested in networked capabilities to support joint and coalition training and experimentation. For example, the U.S. Joint Training and Experimentation Network, is meant to provide a persistent global network for realistic training across the U.S. services and connect to multinational partner and experimentation networks [22]. NATO, likewise, employs a NATO Education and Training Network to integrate member state capabilities across the alliance, while likewise, providing education and training capabilities to NATO operational and tactical headquarters staff who may be preparing to execute NATO missions [23]. The NATO Education and Training Network draws on a persistent networking infrastructure, distributed training and education tools, and standard operating procedures to support NATO headquarters staff training and training activities across the alliance. While the U.S. network and the NATO Education and Training Network are worthwhile goals, connectivity will always prove to be a challenge, particularly for training scenarios that may require high bandwidth, low latency, and continuous connections.

Like joint and multinational training and experimentation events, metaverse experiences are meant to be shared experiences. For the metaverse to be a shared real-time experience, every participant within the metaverse must have a fast, uninterrupted, and continuous high-bandwidth internet connection that is capable of transmitting mass amounts of data between the user and the metaverse's server infrastructure. The human threshold for latency is incredibly low. For a user to feel that they have real agency and presence, a user must feel as if their inputs into the metaverse have real effect—that the virtual world is not responding to inputs well after they are made. The gaming industry has developed partial solutions to the latency dilemma. For instance, games can match and cluster users in similar geographic locations so that data does not have to travel as far between users. However, partial work solutions, such as geographic clustering, will not be adequate for metaverses that span the globe and tap into a global workforce [7].

Latency is the greatest networking obstacle to achieving the metaverse. At present, very few services and applications used today via the Internet—from Netflix to video games or Zoom—require ultra-low latency. As a result, in the near-term incentives do not exist for network operators or technology companies to prioritise real-time delivery of data and services—present technical approaches meet most user needs. However, as commercial interest in the metaverse increases, investments in lower-latency internet infrastructure will grow to meet the demand. These investments will naturally serve the defence M&S community, as distributed training and experimentation will benefit from higher-bandwidth and lower-latency solutions.

2.7 Compute

Any simulated environment needs to be hosted from a compute standpoint. Hosting can take place on a public cloud, a private cloud, an on-premises bare-metal server, or via edge devices, such as a VR headset [24]. In a defence M&S context, the emergence of hybrid clouds have allowed militaries to leverage the security benefits of a private cloud or on-premises infrastructure, while simultaneously utilising the scalability benefits of a public cloud for their virtual training, experimentation, or test and evaluation environments. The use of cloud services for hosting and compute provides immense performance benefits to defence M&S. Indeed, by dispersing computer processing across hundreds, if not tens of thousands of machines, multiple simulations can be run concurrently and in seamless coordination, facilitating more persistent virtual environments with greater fidelity and larger concurrent user counts. At present, however, no defence M&S tool, and no commercial game, demonstrates full persistence, real-time rendering, or high-user concurrency rates. Yet efforts are being made to solve each of these issues as they are essential for achieving a metaverse.

1) **Persistence:** No simulation or commercial game on the market has achieved full persistence. Current solutions run for a finite time-period before resetting to reduce complexity [7]. The more information that persists in a virtual game or a virtual military training event, the greater the computational needs; and as a result, less memory will be available for other activities. Current conceptions of a metaverse imagine a fully persistent world, much like the physical world. This requires immense computational demands, as the world would not only have to persist, but it would also have to evolve. For instance, if a user were to cut down a virtual tree on their virtual property, that tree may need to virtually degrade—it would not necessarily disappear. Achieving full evolutionary persistence will require far more intensive computational power than is currently in use in any simulation or gaming application.

2) **Real-Time Rendering**: Experiences set in a metaverse require real-time 3D rendering—users must be able to see and experience computationally intensive digital media in a dynamic real-time environment. A lag in real-time rendering in a virtual environment can cause feelings of motion sickness among users. Or worse, a lag in rendering can lead to misunderstandings among immersed participants—a particularly problematic proposition in a military context, as it can lead to negative training in various discrete tactical or operational contexts. While this problem can partially be resolved using data centres, issues associated with latency and bandwidth will persist. As a result, efforts are being made to push compute further towards edge devices, like user interfaces, such as XR devices.

3) **User Concurrency**: User concurrency (having a high number of concurrent users in one simulated environment) is a foundational challenge for the metaverse and is also a problem for defence M&S, particularly when simulating complex military manoeuvres at the brigade level or above that may involve many participants. High user counts lead to exponential increases in the amount of data that must be processed, rendered, and synchronised per unit in time [7]. In typical commercial games, when too many players converge on a single place, the simulation will typically “shard”—it will split into concurrently operating but independent copies of that place. In a metaverse, sharding can detract from feelings of presence, particularly when attempting to simulate experiences that are meant to involve many users, like large sports games or concerts. Commercial companies have attempted to solve this dilemma by focusing on increasing the number of operations per second within a simulated environment, while also operating at variable levels of fidelity, depending on game needs [16].

To achieve the computational requirements of a metaverse, some have argued that commercial entities must push as much processing and rendering capabilities as possible into commercial grade data centres. By renting access to cloud facilities, metaverses will then have access to enterprise grade equipment that is more cost efficient per unit of processing power. However, others have argued that the increased employment of data centres will place us at the “wrong side of the latency wall” [7]. According to this school of thought, as local computing power in edge devices increases, that computational power should be leveraged for the metaverse [25]. Should edge devices become computationally more powerful, opportunities exist for the defence M&S community to draw on those advancements for their own needs—particularly for training, test and evaluation, or experimentation applications that require point-of-need solutions.

3.0 THE APPLICATIONS OF THE METAVERSE IN DEFENCE

3.1 Metaverse Applications in Defence M&S Domains

It’s impossible to predict exactly how the metaverse will develop, let alone identify how it will affect defence modelling and simulation. It is possible, however, to propose credible hypotheses by examining parallels in other industries and projecting how they might affect defence. This section explores how metaverse technologies could affect defence M&S tools in the traditional application areas of M&S, as laid out in the NATO Modelling and Simulation Master Plan [26]. It then considers how these technologies may transform defence activities more broadly by enabling rapid adaptation and personnel management practices within NATO member states and across the broader alliance.

Figure 3-1 below shows the application areas for modelling and simulation outlined in the NATO Modelling and Simulation Master Plan [26] plotted schematically on two axes representing two of the factors that make M&S most challenging to apply with confidence: the *complexity* of the subject being modelled or simulated, and the *urgency* with which a model or simulation is required to be set up and used.

The *complexity* of the subject is defined here using the four levels of the *Cynefin* concept [27]: Simple, Complicated, Complex and Chaotic. The more complex the subject, the more complex and flexible the M&S needs to be. Simple tasks can make use of simpler, repeatable synthetic environments, whereas Complicated tasks will need synthetic environments composed from multiple models and multiple data sources. Complex tasks will need M&S to adapt as humans explore and ideate around complex unknown phenomena, and Chaotic tasks are at or beyond the limits of analytical endeavour.

The *urgency* with which a model or simulation is required to be set up and used is shown as a very rough logarithmic timescale from decades through to milliseconds. Urgency drives the degree to which automation may be required and hence creates demands for both the simplification and validity of M&S. Those challenges that are less urgent enable more experimental approaches with far greater human involvement to deal with uncertainty.

These two factors combined map out a space where M&S could be used. However, not all of this space is equally feasible. The current state of M&S (and particularly our ability to compose and gather data for synthetic environments) means that there is sufficient time for M&S to be used with *confidence* to support applications at the bottom left of Figure 3-1, but there is insufficient time available to use M&S with confidence for those applications at the top right. Confidence here is caused by a combination of the rigour and robustness of M&S, its coverage of all the important parts of the challenge, and the degree to which the user can understand and make use of the outputs of the M&S.

Each M&S application area is shown in Figure 3-1 as a continuum that cuts across various levels of complexity and urgency. For example, training personnel on a simple repeatable task might be achieved in hours, days or even weeks, but training leaders to be adaptive and responsive in the face of complex operations likely takes years or even decades.

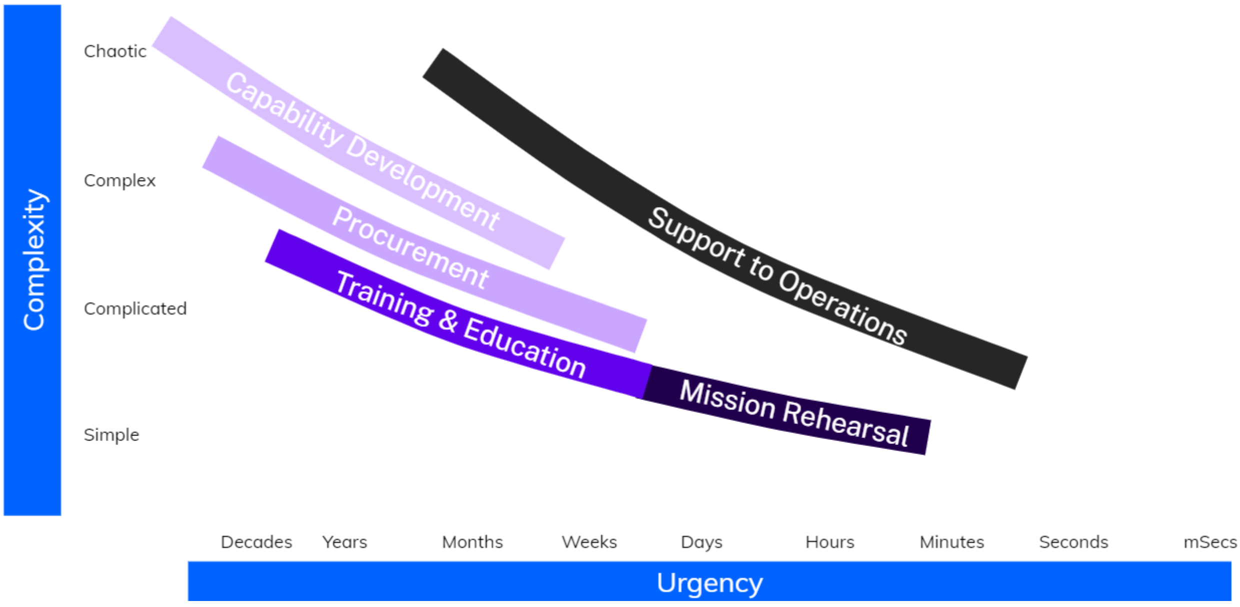

Figure 3-1: Modelling and Simulation Application Areas

3.2 Capability Development

Capability Development (developing policies, strategies, force structures, and concepts of operation) is shown at the top-left of Figure 3-1. Activities that support capability development are complex and can be highly uncertain. As a result, the outcomes of M&S can take years or decades to manifest. The goal is for policymakers, strategists, and planners to assess how the armed forces may be employed in the future. When forecasting far into the future, there is enormous uncertainty from a capability development standpoint. It is impossible to have complete clarity on what various capabilities will be required to achieve, where, why and with whom, how, and finally, against whom. This complexity is further exacerbated because every capability must be adjudicated against other potential capabilities that may be in similar or even adjacent and competing domains. Supporting decisions on which capabilities to develop requires M&S to compare diverse forces operating in a wide range of potential futures and this often takes years with large teams looking at different aspects of the problem, using a wide range of models and simulations. Even when large capability decisions have been made, they often must be refined in more detail, requiring the application of additional models and simulations to help capability planners develop, test, and refine their concepts.

To constrain the complexity of these problems to manageable levels, much of this M&S work is undertaken in silos within NATO member states, and often separately by individual services, or capability branches of those services. Models and simulations tend to be specialised for the silos in which they are designed, often with bespoke representations of similar phenomena—such as line of sight or detection algorithms—and with bespoke datasets of common information, like terrain. Due to the bespoke nature of capability development, there is very little ability to model and understand the interactions between systems that fall across different silos or domains and models and data are often duplicated at great expense across services, various member states' interagency processes, and the alliance as a whole.

A combination of the metaverse components described in Section 2 could allow some of the silos in which capability development takes place to break down—further enhancing interoperability across services and member states within NATO. While it is unlikely that a single, predictable, and detailed NATO metaverse "model of everything" with cascading effects across every domain will ever exist, it is possible that metaverse technologies will offer the alliance the capacity to rapidly develop virtual worlds that “model what matters most” to particular customers. These “metaverses” will be broadly consistent across each virtual world due to the re-use of content, but will likely remain relatively constrained in their complexity to enhance understanding through explainability, while also ensuring speed of composition through their runtime. This coherence between models for different customers should bring greater coherence to those customers, and to their work. As a result, planning for one nation’s naval capabilities could be well-informed by ongoing planning for another nation’s air capabilities and vice versa. Another major benefit of this approach could be coherence across the capability development process—from early ideational wargames into more rigid simulations and large-scale experiments. Indeed, a metaverse that serves NATO, if it is truly a series of seamlessly interconnected virtual worlds, could make a reality of what the godfather of modern wargaming, Peter Perla, labels a “cycle of research”—a cycle whereby one seeks to understand problems and their solutions through iterative wargames, simulations, experiments, analysis, and other methods [28] [9].

Table 3-1: Opportunities posed by a defence metaverse for Capability Development

Metaverse component	**Opportunities for Capability Development**
User Interface	More intuitive visual interfaces enable faster exploration and enhanced understanding, and drive **faster decisions**.
Cyber Physical Interface	M&S updated and calibrated using real-time data, which drives greater realism, validity, and **greater confidence in decisions**.
Runtime	Faster composition of content drives faster analysis, and hence, **faster decisions**. Explainable composition of content drives **greater confidence in decisions**. Greater integration of models, data and outputs enables greater auditability of decisions and hence drives **greater confidence in decisions.** Faster runtimes allow greater exploration of the problem-space, driving **greater confidence in decisions.** Faster runtimes allow the employment of models that simulate **greater complexity**, enabling **more integrated** multi-domain capability development.
Content Ecosystem	A marketplace of small suppliers enables content reuse and encourages continuous improvement of content. This drives **cheaper** M&S development and faster M&S development, which enables **faster decisions**.
Compute	Distributed compute drives faster runtime and, as a result, faster analysis which enables **faster decisions**. Faster runtime allows greater exploration of the problem-space, driving **greater confidence in decisions.** Faster runtime allows the employment of models that simulate **greater complexity**, enabling **more integrated** multi-domain capability development.
Networking	Multiple users are able to view the same M&S, which enables shared understanding. Democratised analysis: multiple users are able to experiment together and in parallel, which increases collaboration and cross-referencing between capability planners. This

	enables **more integrated** (multi-domain) capability development, **greater confidence in decisions,** and **greater agreement on decisions**.
Distributed Ledger	Distributed ledger leads to enhanced security, allowing greater trust in model and data provenance, and hence trust in the validity of outputs, leading to **greater confidence in decisions**.

Some of the opportunities posed by a defence metaverse for capability development are shown in Table 3-1. The key themes emerging are:

- **Faster capability development decisions through**
  - accelerating the process of developing, reusing, composing, running, and understanding the outputs of M&S
- **Greater confidence in capability development decisions through**
  - secure real-world data updating and calibrating M&S in real-time
  - more secure, auditable, explainable data pathways from content, through composition to outputs
  - faster runtime allowing greater exploration of the problem-space
  - networking and interfaces allowing users to view, collaborate and explore models together
- **More complex and integrated capability development decisions through**
  - networking and interfaces allowing users to view, collaborate and explore models together, enabling shared understanding and democratised analysis
  - faster runtime allowing the employment of models of greater complexity
- **Cheaper M&S through**
  - a rich content ecosystem that would allow for greater re-use of models and data

3.3 Procurement

Once a decision has been made on what capability is required, modelling and simulation is widely used to choose, design, test, and build military equipment as part of the procurement process. Procurement decisions, shown in the mid-left of Figure 3-1, are relatively complex and slow. These decisions range from Complex ones taking years (for example, choosing between or designing intricate systems such as submarines) to Complicated ones taking days or weeks (for example, choosing a small commercial-off-the-shelf part or refining the design of a small component). As with capability development, much of this work is necessarily constrained for reasons of simplicity, meaning that systems are designed and tested in relatively narrow situations. Design is often done manually with testing undertaken by a mixture of virtual and live test and evaluation. The process can take years to complete.

Some of the technologies associated with the metaverse are already being embraced to accelerate procurement. One digital engineering approach in particular, model-based systems engineering, has helped to increase the speed of design and development of major weapons systems [29]. For example, the US Air Force's Ground Based Strategic Deterrent megaproject is employing model-based system engineering to rapidly evaluate billions of scenarios, helping acquisition professionals to determine the precise design and placement of munitions in nuclear silos as they work to replace the land-based leg of America's nuclear triad [30]. The program offers a powerful success story for digital engineering and has now become the standard practice on all large US Air Force programs [31]. Yet, these digital versions of complex weapons systems stop short of interacting with each other. They also are rarely integrated into simulations that replicate the complexity of future competition and conflict. A defence metaverse offers the possibility of connecting virtual environments for procurement with those used for capability development or training, allowing procurement professionals to quickly test and evaluate their designs in a virtual world that mimics the future operating environment, all while providing a modicum of operational security that the live environment may not afford [32]. This should support further design and security improvements, while shortening iteration cycles of requirements development, architecture designs, and testing [8] [33].

Perhaps most exciting is the opportunity to replace the standard customer-supplier procurement model, whereby companies are asked to compete for requirements by developing stovepiped solutions, with flexible software development practices. A defence metaverse could foster co-creation through an interactive process of solution design and development. Government customers could pose challenges in the form of scenarios set up in simulations that users could iterate on. This approach could help cohere and accelerate the procurement process vertically (allowing customers to quickly explore innovative ideas with suppliers, and likewise, giving suppliers a much better understanding of customers' needs). It could also horizontally accelerate the process (enabling suppliers to collaborate and build on each other's designs). As a result, this could dramatically speed up the design process for new systems and help governments move from siloed procurement of individual systems, designed to fit into a specific slot in the force structure, to the simultaneous procurement of systems-of-systems with the designs for multiple systems evolving simultaneously.

Table 3-2: Opportunities posed by a defence metaverse for Procurement

Metaverse component	**Opportunities for Procurement**
User Interface	More intuitive visual interfaces enable faster exploration and enhanced understanding, which drives **faster decisions**.
Cyber Physical Interface	Design digital twins updated and calibrated using real time data from prototype sub-systems, which drives greater realism, validity, and **greater confidence in decisions.** This provides a **cheaper and faster test and evaluation** process to test designs and find design flaws before building and trialling the system in live ranges. Production digital twins enable real time monitoring and optimisation of the production process, which drives **cheaper and faster production**.
Runtime	Faster composition of content drives faster analysis, and hence, **faster decisions**. Explainable composition of content drives **greater confidence in decisions**. Greater integration of models, data and outputs enables greater auditability of decisions and hence drives **greater confidence in decisions.** Faster runtimes allow greater exploration of the problem-space, which drives **greater confidence in decisions.** Faster runtimes allow the employment of models that simulate **greater complexity**, which enables **more integrated** multi-domain system-of-systems procurement.

Content Ecosystem	A marketplace of small suppliers enables content reuse and encourages continuous improvement of content. This drives **cheaper** M&S development and faster M&S development, which enables **faster decisions**.
Compute	Distributed compute drives faster runtime and, as a result, faster analysis which enables **faster decisions**. Faster runtime allows greater exploration of the problem-space, which drives **greater confidence in decisions.** Faster runtime allows the employment of models that simulate **greater complexity**, which enables **more integrated** multi-domain equipment development.
Networking	Multiple users are able to view the same M&S, which enables shared understanding and **greater collaboration** between customers and suppliers, and leads to faster resolution of requirements, and **greater confidence in decisions**. Democratised analysis: shared experimentation between multiple suppliers enables simultaneous development of multiple systems, and leads to **faster design** of **more integrated systems of systems**.
Distributed Ledger	Distributed ledger leads to enhanced security, allowing greater trust in model and data provenance, and hence trust in the validity of outputs, which leads to **greater confidence in decisions**. Enhanced security enables **greater collaboration** between companies that are normally competitors, without sharing all the workings of their digital twins, which leads to development of **more integrated systems of systems**.

Some of the opportunities posed by a defence metaverse for procurement are shown in Table 3-2. In addition to the key themes for capability development, two new themes emerging are:

- **Cheaper and faster design, test and evaluation, and production of defence equipment through**
    - a synthetic process to test designs and find design flaws before building and trialling the system in live ranges
    - a cyber physical interface connecting production digital twins to real systems and their production facilities enabling real time monitoring and optimisation of the production process
    - networking and interfaces allowing customers and suppliers to view the same M&S simultaneously, leading to faster resolution of requirements

- **Development of more complex and integrated systems of systems through**
    - enhanced security enabling greater collaboration between companies that are normally competitors, working on simultaneous design of connected systems without sharing all the workings of their digital twins

3.4 Training and Education

Despite the huge effort expended in the procurement of equipment, people play just as important a role in the generation of military capability. The development of people takes place through recruitment, training, education, management, and leadership, all of which are supported to some extent by M&S. Training, however, is by far the greatest consumer of M&S. Training people to develop the skills to undertake Simple to Complicated tasks can take hours, days, or even weeks, whereas education over months or years may be necessary to ensure people can effectively undertake Complex challenges. As such, training and education is shown in the mid-left of Figure 3-1.

It is possible to argue that the armed services have been employing various training metaverses, albeit clunky and siloed ones, for years [17]. The military has been stitching together virtual worlds for the purposes of training since the 1980s when it first created SIMNET (short for "simulator networking"), which was the first demonstration of an extensive simulator network for collective training and mission rehearsal [34]. In the last two decades, standards like DIS and HLA have facilitated the integration of disparate training simulations, allowing warfighters to experience the "fog and friction" of combat within one synthetic space [15]. While this kind of training has been undeniably useful, the integration of differing types of virtual and constructive training has long been imperfect— many of these applications have been designed as monoliths, with modularity or interoperability as an afterthought [17] [35]. However, even with current interoperability challenges, a significant portion of the training community still aspires to a distant future reminiscent of *Ender's Game*, where warfighters can seamlessly train in a realistic immersive world. In some respects, this mirrors current conceptualizations of a metaverse, so it is no surprise that a natural leap has been made from virtual training to a metaverse in defence [36] [9].

In the commercial world, education has been flagged as one area that is ripe for disruption via a metaverse. Educators and commercial innovators imagine experiential opportunities where instead of learning about military history via classic pedagogical approaches, defence students get to witness or partake in battles firsthand [37]. NATO is not immune to this line of thinking, and indeed, could benefit from the integration of metaverse technologies. NATO currently has seven "bricks-and-mortar" education facilities under its control—the NATO Defense College in Rome, Italy; the NATO School in Oberammergau, Germany; the NATO Maritime Interdiction Operational Training Centre in Souda Bay, Greece; the NATO Communications and Information Academy in Oeiras, Portugal; the Joint Warfare Centre in Stavanger, Norway; the Joint Force Training Centre in Bydgoszcz, Poland; and the Joint Analysis Lessons Learned Centre in Lisbon, Portugal [38]. While valuable, as the Covid-19 panic laid bare, bricks-and-mortar institutions will fall short of learning needs across the alliance. Education institutions need to increase opportunities for distributed learning, allowing warfighters and commanders to access valuable education opportunities at their point of need. This could be extended by allowing personnel to learn through exploration, using wargames and faster-than-real-time tools developed for capability development and procurement, in addition to experience gained through real-time training systems. Experiential opportunities have been shown to be of particular value as they increase learner performance [39]. Metaverse technologies could increase those experiential options across the alliance, while also providing tailored feedback to individuals. Moreover, cross alliance learning data could provide valuable metrics to iterate on course syllabi, wargames, and simulations to ensure learning opportunities meet educational goals.

Table 3-3: Opportunities posed by a defence metaverse for Training & Education

Metaverse component	**Opportunities for Training & Education**
User Interface	More intuitive visual interfaces enable faster exploration and enhanced understanding, which drives stronger learning retention and hence **greater confidence in training**. More realistic immersive interfaces bridge the sim-to-real gap and instil belief in the trainee, which drives **faster learning**.
Cyber Physical Interface	Connecting digital twins to real systems increases validity of education for engineers and users on how military systems work, fail, and are operated and repaired, which drives **greater confidence in training**. This provides **cheaper and repeatable training** processes for engineers.
Runtime	Faster composition of content enables **rapidly tailored training**. Faster runtimes enable greater exploration (learning by doing), and hence **greater depth of learning**. Faster runtimes allow the employment of models that simulate greater complexity, which allow **more integrated** training on multi-domain operations.
Content Ecosystem	A marketplace of small suppliers enables content reuse and encourages continuous improvement of content. This drives **cheaper** M&S development and faster M&S development, which enables **faster training development**. Content bridging the gap between wargaming and simulation enables **greater depth of learning** through exploration and learning through doing.
Compute	Faster runtime allows greater exploration of the problem-space, which drives **greater depth of learning.** Faster runtimes allow the employment of models that simulate greater complexity, which allows **more integrated** training on multi-domain operations.
Networking	Multiple users able to view the same M&S enables shared understanding, **greater collaboration** and **enhanced collective training**, even when operating remotely. Networking enables self-teaching through experimentation and exploration. Shared between multiple teams, this enables simultaneous development of tactics and skills leading to **development** of **more integrated teams**.
Distributed Ledger	Distributed ledgers able to securely track the performance of individuals through life, allow tailored training against individual needs, and hence **greater depth of learning**.

Some of the opportunities posed by a defence metaverse for training and education are shown in Table 3-3. In addition to the key themes for the previous application areas, three new themes are emerging:

- **Cheaper and faster training**
    - through more realistic immersive interfaces bridging the sim-to-real gap and instilling belief in the trainee
    - through faster composition of content enabling rapidly tailored training
- **Greater depth of learning and confidence in training**
    - through intuitive visual interfaces, content bridging the gap between wargaming and simulation, and faster runtimes all enabling personnel to enhance understanding through faster-than-real-time exploration of a challenge, driving stronger learning retention
    - through a cyber physical interface connecting digital twins to real systems increasing validity of education for engineers and users on how military systems work, fail, and are operated and repaired
    - through distributed ledgers enabling secure tracking of the performance of individuals through life, allowing tailored training against individual needs.
- **Development of more integrated teams**
    - through faster runtimes allowing the employment of models that simulate greater complexity, allowing more integrated training on multi-domain operations
    - through networking and interfaces allowing users to view, collaborate and explore models together enables shared understanding and enhanced collective training, even when operating remotely

3.5 Support to Operations

Models and simulations are used to support operations by helping intelligence analysts make sense of data provided by intelligence systems, helping planners to develop and test plans in planning systems that are then communicated through command and control systems, and helping operators achieve their objectives through combat systems.

The decisions made on operations can be just as complex as those made in other application areas such as capability development, with commanders facing huge uncertainty in highly fluid situations. From a modelling and simulation standpoint, these are by far the most challenging areas to support because they are much more urgent than other decisions of a similar complexity. The support to operations application area is shown as a line in Figure 3-1, ranging from tactical decisions at the bottom right to strategic decisions in the top middle of the figure.

- Although tactical decisions are often Complicated problems, meaning they can be solved with quite high confidence using variations of existing analytical approaches, they are also the most urgent, sometimes needing to be made in minutes or seconds. As a result, there is very little time for humans to set up, run, and interpret M&S to aid these decisions. Instead, M&S is primarily used in advance of operations to provide data sets and simple rules or heuristics that can be included in combat systems or taught to personnel through training. Sometimes M&S is used as part of the combat systems themselves, for example to improve weapon targeting.

- There is more time available to support Complex operational level decisions, maybe days or weeks, but even in this timescale there is very rarely time for humans to develop and iterate models able to capture the complexity of operational issues. Instead, planners are sometimes supported by intelligence analysts and operational researchers specially trained to operate under substantial time pressure and uncertainty, making the most of simple tools and applying them as best as possible to the problem at hand.

- Strategic decisions that need to be made in weeks or months are rarely well-supported by M&S because the Chaotic, fluid and qualitative nature of the challenges they address makes it difficult to build and maintain confidence in the models needed to address them.

In all of these cases, the consequences of success or failure are high, driving a demand for validity and high confidence in the M&S used. This is usually achieved by locking in (testing and evaluating) predictable performance in advance, rather than using real-time feedback to support self-correcting behaviour.

Metaverse technologies offer the opportunity to substantially improve the applicability of M&S in this application area. Real-time data pipelines providing feedback from intelligence sources and numerous sensors in blue (i.e., friendly) systems, connected through a cyber physical interface could enable the continuous refinement, calibration, and validation, of models. This would greatly improve the quality of M&S, and users’ confidence in its applicability to their problems.

The creation of a “cyber physical infrastructure” has been proposed by the UK’s *Robotics Growth Partnership* [11], enabling direct connection of numerous civilian systems and their digital twins. A NATO-wide version of this could enable the delivery of the NATO Network Enabled Capability concept of 20 years ago, which was arguably ahead of the technology required to deliver it [40].

Other metaverse technologies, particularly user interfaces and networking, could significantly enhance human involvement in intelligence, planning, and operations by facilitating the real-time collaboration of multiple distant users rather than users operating in isolation and merging their work periodically. This could lead to enhanced teamwork through everyone visualising and annotating the same information from their own perspective, creating shared understanding, and facilitating the communication of different mental models and plans. Capabilities similar to these are already being developed for a range of civilian applications, including the business, gaming, and entertainment sectors, and the authors’ company has demonstrated that these benefits translate well to an operational decision support tool for military planners [41]. The same technologies could also enable planners to see the situation from the perspective of their adversaries. Integrated wargaming and simulation could then be employed to test plans and ensure their robustness against those same identified threats. Finally, a convergence of artificial intelligence, data science, and simulation could enable artificial intelligence to perform a far more useful role as an intelligent adviser to decision makers, enabling them to develop true cognitive advantage [42].

Table 3-4: Opportunities posed by a defence metaverse for Support to Operations

Metaverse component	**Opportunities for Support to Operations**
User Interface	More intuitive visual interfaces enable faster exploration of risks and alternative situations, which drives **greater confidence in plans**. More realistic immersive interfaces bridge the sim-to-real gap and instil belief in the user, driving **faster planning**.
Cyber Physical Interface	Connecting M&S to command and control and intelligence systems drives greater validity, and **greater confidence in plans.** Tactical plans directly transferred to autonomous systems, drives **faster planning**.
Runtime	Faster composition of content enables more tailored testing of plans, which enables **greater confidence in plans**. Faster runtimes enable greater exploration of risks and alternative situations, which drives **greater confidence in plans**. Faster runtimes allow the employment of models that simulate **greater complexity**, which enables **more integrated** planning for multi-domain operations.
Content Ecosystem	A marketplace of small suppliers enables content reuse and encourages continuous improvement of content. This drives **cheaper** M&S development and faster M&S development, which enables more up to date M&S to test plans, which drives **greater confidence in plans**. Content bridging the gap between wargaming and simulation enables **greater confidence in plans** through exploration. Content at the convergence of AI, data science and simulation enables AI advisers to planners, which brings **greater confidence in plans**.
Compute	Distributed compute drives faster runtime and, as a result, greater exploration of the problem-space, driving **greater confidence in decisions.** Faster runtime allows the employment of models that simulate **greater complexity**, enabling **more integrated** plans for multi-domain operations.
Networking	Multiple users able to view the same M&S enables shared understanding and **greater confidence in plans**, as well as the **development** of **more integrated plans**.
Distributed Ledger	Distributed ledger leads to greater robustness under attack and greater trust in model and data provenance and hence in the validity of outputs, leading to **greater confidence in plans**.

Some of the opportunities posed by a defence metaverse for support to operations are shown in Table 3-4. In addition to the key themes for the previous application areas, two new themes emerge:

- **Faster translation of intelligence into plans into actions through**
    - M&S connected by a cyber physical interface to command and control and intelligence systems enabling direct transfer of intelligence into plans and of plans into autonomous systems
- **Greater confidence in plans through**
    - connecting M&S to command and control and intelligence systems driving greater validity
    - AI advisers through the convergence of AI, data science and simulation content

3.6 Mission Rehearsal

Mission rehearsal can be seen as a special case of training and education with the user receiving urgent preparation tailored to specific missions, as opposed to less urgent, and more generic training and education designed to prepare for a range of future mission sets. As such, many of the same issues affecting training apply equally to mission rehearsal. However, the time-sensitive and bounded nature of mission rehearsal means that it is shown in the lower middle of Figure 3-1. With mission rehearsal, a plan has been developed and there may be insufficient time to explore alternative options.

Metaverse technologies, such as faster runtimes, compute and tooling for synthetic environment composition could enable faster development of scenarios and models for mission rehearsal. This could result in increased time for rehearsal or a greater accuracy, and hence, confidence in the M&S used for rehearsal. In addition, partial automation of elements of the rehearsal process could enable participants to focus on those scenarios deemed to require the majority of their time (perhaps those with highest risk), while allowing artificial intelligence to run constructive simulations (i.e. without human input in the running of the simulation, hence able to run much faster than real time) and then highlight key lessons to the user.

Table 3-5: Opportunities posed by a defence metaverse for Mission Rehearsal

Metaverse component	**Opportunities for Mission Rehearsal**
User Interface	More intuitive visual interfaces enable faster exploration of risks and alternative situations, which drives **greater confidence in preparation**. More realistic immersive interfaces bridge the sim-to-real gap and instil belief in the user, driving **faster preparation** and potentially offering **greater confidence in preparation** to provide improved inoculation to combat stress from the mission.
Cyber Physical Interface	Connecting M&S to command and control and intelligence systems drives greater validity, and **greater confidence in preparation**.
Runtime	Faster composition of content enables more tailored mission rehearsal, which enables **greater confidence in preparation**. Faster runtimes enable greater exploration of risks and alternative situations, which drives **greater confidence in preparation**. Faster runtimes allow the employment of models that simulate **greater complexity**, which enables **more integrated** preparation for multi-domain operations.
Content Ecosystem	A marketplace of small suppliers enables content reuse and encourages continuous improvement of content. This drives **cheaper** M&S development and faster M&S development, which enables more up to date M&S for mission rehearsal, which drives **greater confidence in preparation**. Content bridging the gap between wargaming and simulation enables **greater confidence in preparation** through exploration.
Compute	Distributed compute drives faster runtime and, as a result, greater exploration of the problem-space, driving **greater confidence in preparation.** Faster runtime allows the employment of models that simulate **greater complexity**, enabling **more integrated** preparation for multi-domain operations.
Networking	Multiple users able to view the same M&S enables shared understanding and **greater confidence in preparation**, even when operating remotely, as well as the **development** of **more integrated teams.**
Distributed Ledger	Distributed ledger leads to greater robustness under attack and greater trust in model and data provenance and hence in the validity of outputs, leading to **greater confidence in preparation**.

Some of the opportunities posed by a defence metaverse for mission rehearsal are shown in Table 3-5. One additional key theme emerges compared to the previous application areas:

- **Greater confidence in preparation through**
  - more realistic immersive interfaces providing improved inoculation to combat stress from the mission.

3.7 Future Military M&S Applications: Expanding Beyond Traditional M&S Domains

Just as mission rehearsal can be seen as a special case of training and education, where training and education provides people with a general preparation for future missions, but mission rehearsal supplements this by being tailored to a specific and urgent requirement, Figure 3-2 shows three similar special cases of urgent, tailored, capability development, procurement, and support to operations. In each of the cases highlighted below, M&S will increasingly support NATO members as metaverse technologies evolve:

- Rapid adaptation of capability (where M&S can be used to adapt how in-service forces are used and configured)

- In service support (where M&S can be used to manage, and optimise how in-service military systems are used and configured)

- Autonomy (where M&S forms a vital part of the control system of individual systems and groups of systems, controlling how they are used and configured)

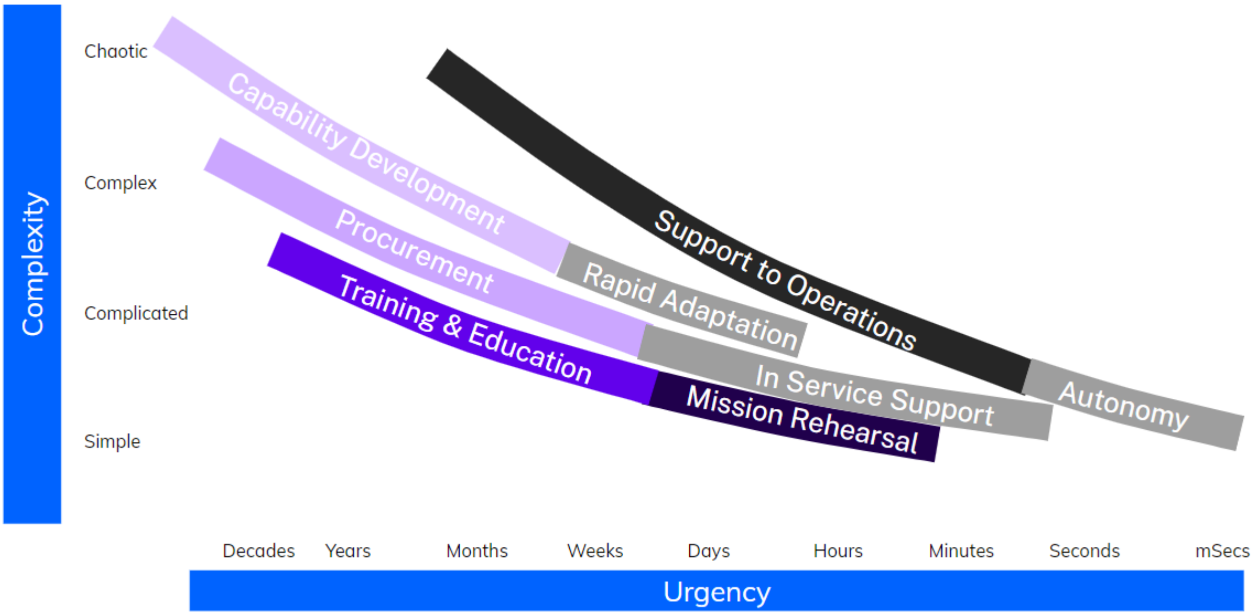

Figure 3-2: Additional Modelling and Simulation Application Areas

3.7.1 Rapid adaptation of capability

The rapid adaptation of forces has long been a goal of militaries, but it is extremely challenging due to the slow pace of capability development. Metaverse technologies will not overcome all the challenges tied to capability development, but they could enable a new way of developing (or enhancing) capability through rapid adaptation in concepts of use or tactics. Rapidly changing the way in which military systems are used, configured and integrated offers an opportunity to surprise an adversary, and it can easily be experimented on through wargaming and simulation. Opening a defence metaverse to many defence professionals, companies, and academics (and maybe even the public) creates the possibility of democratising capability analysis, theoretically bringing thousands of minds into an innovation ecosystem in support of NATO. The task of adapting the armed forces in line with the best ideas will still be challenging, but the chances of developing better and more surprising ways of operating could be substantially improved.

3.7.2 In service support

Much of today's military expenditure is on the sustainment of capability. M&S is already used extensively in supporting in-service systems, for example in logistics, optimising supply chains and maintenance schedules, or in projecting future operational capability from fleets. This capability stands on the brink of substantial enhancement through the widespread use of digital twins to forecast the performance of these systems, and through linking these via a cyber physical interface to real world system performance data from a network of sensors. Extending this network further through a cyber physical infrastructure [39] could enable optimisation across whole networks of systems, for example by optimising the allocation of tasks between systems to minimise the risk of failures of specific parts or systems leading to failure of the overall mission.

3.7.3 Autonomy

The "support to operations" application area is predominantly focused on M&S run by expert analytical users supporting human decision makers. As described above, metaverse technologies could enhance the speed and complexity of this enterprise, with networking, shared information and distributed planning tools using edge compute, thereby enabling the concept of mosaic warfare or multi-domain integration, making NATO forces far more robust and adaptable. Metaverse technologies also have the potential to lower the threshold at which decisions are currently deemed safe to delegate to a machine. Detailed models are already embedded in many military systems as part of their real-time automated control systems. For example, algorithms predicting the trajectory of a projectile are used to aim weapon systems. The process of validating and testing these algorithms, however, is extremely slow.

The increased speed of M&S composition and development, combined with continuous validation (and hence continuous improvement) of those simulations with real-time data pipelines, could greatly accelerate the process of validation and acceptance into service for algorithms used in control systems. In addition, greater computing power and faster runtimes enabling more robust analysis should also lead to greater confidence in the results of those M&S. Despite this enhanced capacity for improving algorithms, the ethical challenges of releasing autonomous systems that are continuously "improving" themselves will remain a major policy issue.

3.7.4 Personnel Management

Recruiting, retaining, and managing defence personnel are some of the most important activities undertaken by defence forces. But many of the approaches used today are the same ones that have been used for centuries. For example, allocation of personnel to posts is a largely human endeavour, undertaken with limited involvement of personnel themselves and based on personnel records that have been critiqued as inadequate — lacking information on the complexity and breadth of an individual's skills and latent talents. A defence metaverse could integrate and automatically update personnel records with activities that occur elsewhere within the metaverse — from training to experimentation and education. A metaverse may also provide alternative pathways to identify future military leaders (or mavericks) who are uniquely suited to the future fight. Indeed, with the advent of massive multiplayer online role-playing games, corporations noticed that the gaming environment often produced leaders who possessed the types of skills that would be applicable in an enterprise environment: a comfort with risk, a willingness to accept failure, great interpersonal skills, and a desire for iterative and agile improvement [43,44].

As the metaverse is fundamentally a social construction [45], NATO militaries could also use it to provide new opportunities for their members to interact, allowing people to forge new relationships and ideally enhance the social elements of their lives. Just like military bases provide opportunities to socialise and build communities, the metaverse could also provide social activities, from morale, welfare, and recreation programmes to healthcare and financial guidance. For example, players of Fortnite have opportunities to hang out or make friends [46], and now the US Air Force Gaming community [47] has taken a first step towards connecting distributed airmen in a digital environment through video games, providing opportunities for leadership development, teamwork, morale building, and support for the mental health of servicemembers, particularly those in the 18 to 30 age range who grew up as avid gamers. A military metaverse could serve as an extension to this community, bringing in other non-gaming activities and connectivity.

While it is likely aspects of a defence metaverse will be walled off from commercial metaverses (much like how NATO has its own classified networks), interoperability may provide additional benefits. Servicemembers traditionally change duty locations every two to four years — placing pressure not only on the servicemember, but also their families. Spouses often have to find new employment opportunities and children must be enrolled and acclimated in unfamiliar school districts. Commercial or civilian metaverses may allow civilian spouses to maintain their employment, with little to no interruption in professional activities, as they change locations with their military partner. Interconnecting a defence metaverse with commercial metaverses could streamline that process, allowing NATO militaries to quickly provide resources and guidance to civilian professional organisations to ease any needed transition. The children of servicemembers may also be able to maintain linkages with their former academic institutions through immersive hybrid learning opportunities, allowing them to transition to a new location without having to sever former educational contacts or friendships.

3.8 Breaking Silos Across Traditional and Future M&S Domains

Metaverse technology offers the possibility of substantial benefits for each of the traditional M&S application areas and, as discussed above, it will open up several new application areas. But perhaps the greatest benefits will emerge through the interconnection of the various defence virtual worlds, provided interoperability is prioritised in the design of these virtual environments from the start. Integrating virtual activities across NATO should create an iterative feedback loop, ensuring that lessons learned from training, mission rehearsal, or support to operations can be exploited during capability development and procurement and vice versa. As more individuals have access to information across a defence metaverse, potential exists for experiments, analysis and planning, to become increasingly democratised, making it easier to solicit ideas and feedback across the defence community. Even the social facets of a defence metaverse could yield battlefield improvements, by potentially aggregating information that can lend insight into factors like morale that could inform force design or training.

In some ways this mirrors the benefits that platforms like Amazon, YouTube, and Pinterest, provide [48]. By facilitating the development of complementary products and services, platforms generate network effects [49]. The more complementary elements within a platform, the more innovative and powerful the network becomes. In the case of corporations, this has facilitated enormous economic benefits, creating ecosystems in which tremendous amounts of value are created and exchanged. A defence metaverse, much like many platforms, should also facilitate the reuse of M&S, data and solutions, helping to drive down the cost of virtual environments in each application area. For example, force-on-force models that are used for capability development could theoretically be reused in applications for procurement, training and simulation, or support to operations. At present, these are often bought separately, and reuse of M&S and data is often expressed as a requirement, but rarely achieved. Platforms in other sectors have demonstrated that it is possible for information, products, software tools, and services to be widely shared and reused across the platform ecosystem, much like how GitHub has become a repository for open-source software programs or how the Unreal engine has a marketplace for content as well as a games store.

3.9 Risks

Most of the sections above have focused on the opportunities posed by metaverse technologies. But with every new advance in technology comes both opportunity and risk. Metaverse technologies will be no exception. Some of the strengths of the metaverse have corollaries that can be seen as risks. These are shown in Table 3-6, but the primary risks are related to security and safety.

Exploiting the full potential of the defence metaverse will mean concentrating a vast amount of valuable information in one place, making it deliberately accessible to huge numbers of people, and connecting directly to a far-reaching network of physical assets. This will make it the most attractive target for espionage, deception and disinformation. The cyber threat will be extremely high and this threat is likely to be compounded by fallible human users who will likely be unusually susceptible to deception in an unfamiliar environment. Finally, the metaverse, like the internet, may surface and amplify human weaknesses. The negative effects of some social media platforms that enable political polarisation and social fragmentation, amplify disinformation and facilitate harassment have been the subject of substantial discussion over the past few years [50]. A defence metaverse, if properly structured to foster interactions across the military, could reap immense warfighting rewards, but only if it protects its virtual users from some of the toxic behaviours that have plagued the military in the physical realm [51, 52].

All of the above mean that defending, securing and making safe a defence metaverse will be a huge undertaking, but nonetheless one that is likely to be worth the effort, given the potential benefits. NATO should prepare for operations in the metaverse, not only to secure a defence metaverse operated by NATO, but also to defend NATO citizens in their own civilian metaverses. This, in itself, will pose challenging legal questions as to whether protection of citizens extends to their activities and their property in the metaverse. Finally, NATO militaries may find opportunities to achieve effect against adversaries by undertaking offensive operations within metaverses controlled by others.

Table 3-6: Risks posed by a defence metaverse

Metaverse component	Risks
User Interface	Visual interfaces with an expectation of dealing with avatars rather than face to face could make people more susceptible to being fooled by impersonators. Extended use of visual interfaces may lead to fatigue or issues such as motion sickness negatively impacting users. Employment of other sensory interfaces, such as haptics could lead to ethical or health and safety risks needing consideration.
Cyber Physical Interface	Direct access to command and control systems, intelligence systems and control systems of military equipment from a military metaverse could introduce new cyber vulnerabilities in these systems. Spoofing using deliberately incorrect data.
Runtime	The greater capability of runtimes and ability to explore multiple situations could create information that is more valuable to our adversaries as well as us.
Content Ecosystem	Greater concentration of information accessible and modifiable in one place will create cyber vulnerabilities. Any in-built biases, assumptions or inaccuracies will skew outcomes and affect trust.
Compute	Greater attack surface for cyber against servers and ability to run more compute-hungry attacks.
Networking	Direct access to every user creates a greater opportunity to affect many people at the same time. Opportunities for toxic behaviours increase, traceability becomes more complex.
Distributed Ledger	Ledger is shared with and accessible to everyone - hard to modify, but easy to read

4.0 CONCLUSION AND FUTURE DIRECTIONS

The technologies that will underpin the metaverse are developing at a rapid rate for multiple civilian applications. Applying these technologies to create a defence metaverse (or multiple defence metaverses) has the potential to bring substantial benefits.

Increased Urgency, Transformed M&S, Improved Defence Outcomes: M&S will be transformed, becoming cheaper, faster and more effective, leading to improvements in both the speed and rigour of those defence processes and activities which depend on M&S such as: planning and decision making, design, test & evaluation, production, learning, and preparation. In addition, a metaverse will help to cut across traditional stovepipes in these activities and may open up new processes to make NATO more adaptable.

Benefits from Top to Bottom: At the individual level, advances in bridging the sim to real gap and rapidly configurable training programs will enable improved tailoring of learning experiences and therefore improved learning outcomes. At the collective and organisational level, improvements in M&S speed, capability and configurability will improve operational planning and enhance adaptability, accelerate capability development and improve the delivery and effectiveness of collective training.

Increased Confidence, Increased Risk: Although metaverse technologies will provide greater confidence in decisions, training and preparation, there are risks, particularly to security and safety. Metaverse technologies have the potential to increase user confidence in the results of M&S from what has previously been possible, enabling more productive training, capability development and procurement, but also increasing success on the battlefield. But this comes hand in hand with increased risk of espionage, deception and disinformation. Concentrating so much valuable information in one place, making it deliberately accessible to so many people, and connected directly to so many physical assets will make a military metaverse a most attractive target. The cyber threat will be high and this is likely to be compounded by human users perhaps being more susceptible to deception in an unfamiliar environment. Finally, the metaverse, like any other environment for humans to operate within, will be susceptible to human failings. These risks will need to be identified and managed from the outset to maintain trust in the system.

Opportunities for M&S of Greater Complexity to Increase Collaboration and Integration: Metaverse technologies have the potential to greatly increase integration across NATO nations, across domains and across the defence enterprise by democratising M&S in support of multiple applications. Defending, securing and making safe a defence metaverse will be a huge undertaking, but nonetheless one that is likely to be worth the effort, given its benefits. This will also mean that NATO should prepare for operations in the metaverse, not only to secure a defence metaverse operated by NATO, but also to defend NATO citizens in their own civilian metaverses, and to achieve effect against adversaries by undertaking offensive operations within metaverses controlled by others.

There is significant potential for metaverse technology to benefit NATO M&S, with a large number of exploitation paths and opportunities for development. It is time to take a structured approach to developing this concept further, navigating through the various technological options, developing a roadmap in line with desired outcomes and identifying and planning for risks and issues.

5.0 REFERENCES

[1] Jade Scipioni, “How Bill Gates described the internet to David Letterman in 1995: ‘It’s wild what’s going on,’” *CNBC Make it*, 8 December 2019, https://www.cnbc.com/2019/12/08/how-bill-gates-described-the-internet-to-david-letterman-in-1995.html.

[2] Lau Christensen and Alex Robinson, “The Potential Global Economic Impact of the Metaverse,” *Analysis Group* (2022).

[3] David Cotriss, “The Metaverse Economy: Which Industries and Sectors of the Economy will the Metaverse Disrupt?,” *Nasdaq*, 26 July 2022, https://www.nasdaq.com/articles/the-metaverse-economy%3A-which-industries-and-sectors-of-the-economy-will-the-metaverse.

[4] Craig Beddis, “Why Is the Defence Sector Creating the Metaverse,” *The Runway Air Force*, 18 October 2021, https://runway.airforce.gov.au/resources/link-article/why-defence-sector-creating-metaverse.

[5] Turner Wright, “US Air Force files trademark application for ‘SpaceVerse’ initiative,” *Coin Telegraph*, 19 April 2022, https://cointelegraph.com/news/us-air-force-files-trademark-application-for-spaceverse-initiative.

[6] Fabio Vanorio, “Metaverse: Implications for Security and Intelligence,” *NATO Foundation Defense College Paper*.

[7] Matthew Ball, “*The Metaverse: And How it Will Revolutionize Everything*” (New York, NY: Liverright Publishing Corporation, 2022).

[8] Herman Narula, “*Virtual Society: The Metaverse and the New Frontiers of Human Experience*” (New York, NY: Currency, 2022).

[9] Jennifer McArdle and Caitlin Dohrman, “The Full Potential of a Military Metaverse,” *War on the Rocks*, 18 February 2022, https://warontherocks.com/2022/02/the-full-potential-of-a-military-metaverse/.

[10] Leonard Lee, “How to Leverage Internet of Things (IoT) Opportunities in the Metaverse,” *Acceleration Economy*, 17 February 2022, https://accelerationeconomy.com/metaverse/how-to-leverage-internet-of-things-iot-opportunities-in-the-metaverse/.

[11] Department for Business, Energy, & Industrial Strategy, “Robotics Growth Partnership launches cyber-physical infrastructure vision,” *UK Government*, 11 February 2022, https://www.gov.uk/government/news/robotics-growth-partnership-launches-cyber-physical-infrastructure-vision#:~:text=The%20Robotics%20Growth%20Partnership%20(%20RGP,prototype%2C%20test%20and%20develop%20ideas..

[12] Kevin McAllister, “What’s the biggest effect the metaverse will have on IoT, or vice versa?” *Protocol*, 25 January 2022, https://www.protocol.com/braintrust/metaverse-effects-internet-of-things?rebelltitem=20#rebelltitem20.

[13] Arif Furkan Mendi et. al., “Digital Twin in the Military Field,” *IEEE* 26.5 (September-October 2022): 33-40.

[14] Bryan Clark, Dan Patt, and Harrison Schramm, “Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations,” *Center for Strategic and Budgetary Assessments* (2020).

[15] Gabriel Wainer and Khaldoon Al-Zoubi, “An Introduction to Distributed Simulation,” in John Sokolwiski and Catherine Banks, *Modeling and Simulation Fundamentals: Theoretical Underpinnings and Practical Domains* (Hoboken, NJ: John Wiley & Sons, 2010): 373-402.

[16] Rakesh Sharma, “Non-Fungible Token (NFT): What it Means and How it Works,” *Investopedia*, 22 June 2022, https://www.investopedia.com/non-fungible-tokens-nft-5115211.

[17] Jennifer McArdle and Caitlin Dohrman, “From Legos to Modular Simulation Architectures: Enabling the Power of Future (War) Play,” *U.S. Army Mad Scientist Laboratory*, 25 January 2021, https://madsciblog.tradoc.army.mil/299-from-legos-to-modular-simulation-architectures-enabling-the-power-of-future-war-play/.

[18] Emily Rutland, “Blockchain Byte,” *R3 Research* (2017).

[19] Value Technology Foundation, “Potential Uses of Blockchain by the U.S. Department of Defense,” *Value Technology Foundation* (March 2020).

[20] US Congress, “National Defense Authorization Act for Fiscal Year 2020,” *Public Law 116-92* (20 December 2019).

[21] Andrew S. Tanenbaum and David J. Wetherall, *Computer Networks 5th Edition* (Nodia, India: Pearson India Education Services, 2014).

[22] John Kostoff, “Live and Virtual Assets Train Jointly,” *Signal Magazine*, 1 June 2010, https://www.afcea.org/signal-media/live-and-virtual-assets-train-jointly.

[23] MSG-068, “NATO Education and Training Network,” *RTO Technical Report TR-MSG-068* (February 2012).

[24] Erl Thomas et. al., *Cloud Computing: Concepts, Technology, and Architecture* (Upper Saddle River, NJ: Pearson, 2013).

[25] Steven Carlini, “How Edge Computing Will Power the Metaverse,” *Forbes*, 18 May 2022, https://www.forbes.com/sites/forbestechcouncil/2022/05/18/how-edge-computing-will-power-the-metaverse/?sh=5069bb43630d.

[26] North Atlantic Council, *NATO Modelling and Simulation Master Plan: NATO Modelling and Simulation Strategic Plan, Version 2.0* AC/323/NMSG(2012)-015 (14 September 2012): 7.

[27] D.J. Snowden and M.E. Boone. “A Leader’s Framework for Decision Making”. (*Harvard Business Review*, 2007).

[28] Peter Perla, “The Art of Wargaming: A Guide for Professionals and Hobbyists”, (*Annapolis, MD: United States Institute Press*, 1990).

[29] Capital Factory, “Implications of Digital Engineering/ MBSE within the 21st Century,” *Fed Supernova*, 1 April 2021, https://capitalfactory.medium.com/implications-of-digital-engineering-mbse-within-the-21st-century-189f2af88ec9.

[30] Emmett Simmons, "GBSD Powerful Examples Model Based Systems Engineering 3.22.21," *Defense Acquisition University*, 24 March 2021, https://media.dau.edu/media/GBSD+Powerful+Examples+Model+Based+Systems+Engineering+3.22.21/1_txt45lls.

[31] Marisa Alia-Novobilski, "New AFMC office to drive digital transformation across Air, Space enterprise," *US Air Force*, 9 June 2021, https://www.af.mil/News/Article-Display/Article/2650593/new-afmc-office-to-drive-digital-transformation-across-air-space-enterprise/.

[32] Robert Richbourg et. al., "Supporting Joint Warfighting with Mission-Level Simulations," *War on the Rocks*, 16 March 2020, https://warontherocks.com/2020/03/supporting-joint-warfighting-with-mission-level-simulations/.

[33] Alex Blivas and Brenen Tidwell, "Cycle Times and Cycles of Acquisition Reform," *Center for Strategic and International Studies* (5 August 2020).

[34] L. Neale Cosby, "SIMNET: An Insider's Perspective," *IDA Document D-1661* (March 1995).

[35] Andreas Tolk et. al., "How is M&S Interoperability Different from Other Interoperability Domains," *Modeling, Simulation, & Visualization Engineering Faculty Publications* 31 (2012).

[36] Andy Fawkes, "Has the Military Been Building a Metaverse?," *Halldale Group*, 24 November 2020, https://www.halldale.com/articles/17827-has-the-military-been-building-the-metaverse?v=preview.

[37] Kathy Hirsh-Pasek et. al., "A whole new world: Education meets the metaverse," *Brookings*, 14 February 2022, https://www.brookings.edu/research/a-whole-new-world-education-meets-the-metaverse/.

[38] NATO, "Education and Training," 2 June 2022, https://www.nato.int/cps/en/natohq/topics_49206.htm.

[39] Hanan Kondratjew and Marion Kahrens, "Leveraging experiential learning training through spaced learning," *Journal of Work Management* (30 August 2018).

[40] NATO Consultation, Command, and Control Agency, "NATO Networked Enabled Capability Feasibility Study: Executive Summary, Version 2.0," *NATO* (October 2005).

[41] Improbable's Defence business awarded contract for a second year, (*Improbable.io*, 12 November 2020), https://www.improbable.io/blog/improbable-uk-strategic-command-sse

[42] Richard J Carter, "Cognitive Advantage", (*UK: Mayhill Publishing*, 2021)

[43] Mysirlaki S and Paraskeva F, "Leadership in MMOGs: A field of research on virtual teams", *Electronic journal of e-learning Volume 10 issue 2, 2012.* https://files.eric.ed.gov/fulltext/EJ985424.pdf

[44] "Virtual Worlds, Real Leaders: Online games put the future of business leadership on display", *IBM*, (2007), https://www.ibm.com/ibm/files/L668029W94664H98/ibm_gio_gaming_report.pdf

[45] Herman Narula, "Herman Narula on why the metaverse matters", *The Economist*, 22 Nov 2021. https://www.economist.com/by-invitation/2021/11/02/herman-narula-on-why-the-metaverse-matters

[46] "Introducing Fortnite party worlds", *Epic Games*, 2021. https://www.epicgames.com/fortnite/en-US/news/introducing-fortnite-party-worlds

[47] "AF Services Center debuts Air Force gaming", 26 Nov 2020. https://www.af.mil/News/Article-Display/Article/2427781/af-services-center-debuts-air-force-gaming/

[48] Geoffery G. Parker, Marshall W. Van Alstyne and Sangheet Paul Choudary, "Platform Revolution: How Networked Markets are Transforming the Economy and How to Make Them Work for You", (*W. W. Norton & Company*, Oct. 2017)

[49] Michael A. Cusumano, David B. Yoffie, and Annabelle Gawer, 'The Future of Platforms', (*MIT Sloan Management Review*, 11 February, 2020. https://sloanreview.mit.edu/article/the-future-of-platforms/

[50] Brian Friedberg and Joan Donovan, 'The Platform Is the Problem', (*Centre for International Governance Innovation*, 11 Dec 2019). https://www.cigionline.org/articles/platform-problem/

[51] Tanya Basu, "The metaverse has a groping problem already", *(MIT Technology Review*, 16 December 2021). https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/

[52] Joie D. Acosta, Matthew Chinman, Amy L. Shearer, "Countering Sexual Assault and Sexual Harassment in the US Military", *(RAND Published Research).*
https://www.rand.org/pubs/research_reports/RRA1318-1.html