Requirements for Simulation of the Future Operating Environment and Multi-Domain Operations

Per-Idar Evensen, Even Soltvedt Hvinden, Helene Rødal Holhjem,
Daniel Myklatun Tveit, Karolina Di Remigio Eikås
Norwegian Defence Research Establishment (FFI)
Kjeller, Norway
per-idar.evensen@ffi.no, even-soltvedt.hvinden@ffi.no, helene-rodal.holhjem@ffi.no,
daniel-myklatun.tveit@ffi.no, karolina-di-remigio.eikas@ffi.no

ABSTRACT

The future operating environment is expected to become increasingly complex, lethal, and ambiguous. The operational tempo in high-intensity operations is expected to increase, and effects will be increasingly cross-domain and contemporaneous. An essential question is: How can our forces conduct successful military operations in the envisioned future operating environment?

The proposed solution is multi-domain operations (MDO). MDO is an operational concept where the underlying idea is seamless integration of capabilities and activities in all the operational domains (land, maritime, air, space, and cyberspace), to present the enemy with multiple simultaneous dilemmas and achieve overwhelming superiority in time and space on the battlefield. MDO will, however, be inherently much more complex to execute than current operations of the same scale, due to a higher diversity of combat elements and capabilities (from all operational domains), higher requirements for synchronization of capabilities, activities and actions, and higher requirements for operational tempo.

Modeling and simulation (M&S) and wargaming will be essential in experimentation with, and further development and detailing of, the MDO concept. However, M&S of the future operating environment and MDO will also be correspondingly more complex. In addition, very few, if any, of the simulation tools currently available can represent combat elements and capabilities in all operational domains at a sufficient and balanced level of fidelity throughout the combat model.

In this paper we first give a summary of how the future operating environment is envisioned to be like in a 2025–2045 perspective and what technologies are expected to dominate on the battlefield, based on recent literature. Moreover, we provide a description of the concept of MDO, including definitions, historical origin, characteristics, and challenges. Finally, we outline and discuss a set of overall requirements for simulation of the future operating environment and MDO for concept development, experimentation, and analysis.

ABOUT THE AUTHORS

Per-Idar Evensen is a Principal Scientist at the Norwegian Defence Research Establishment (FFI), where he has worked since 2006. His current research work focuses on modeling and simulation (M&S) of multi-domain operations at different levels for experimentation and analysis purposes, and he has published more than a dozen peer-reviewed papers in M&S related conference proceedings and journals. Per-Idar has a Master of Science degree in Computer Science from the University of Oslo in 2004.

Even Soltvedt Hvinden, Ph.D., is a Senior Scientist at the Norwegian Defence Research Establishment (FFI), where he has worked since 2023. His research concerns the measurement of operational performance and economic cost of future force structures. Even has a PhD in Economics from the BI Norwegian Business School in 2021.

Helene Rødal Holhjem is a Principal Scientist at the Norwegian Defence Research Establishment (FFI), where she has worked since 2007. Her current research work focuses on using modeling and simulation (M&S) and simulation-

based experiments to support development of operational concepts. She has a Master of Science degree in Applied Physics from the Norwegian University of Science and Technology in 2007.

Daniel Myklatun Tveit, Ph.D., is a Scientist at the Norwegian Defence Research Establishment (FFI). His research is focused on utilizing modeling and simulation to support experimentation for doctrine development and testing, and to facilitate and analyze live exercises and operations. Daniel was awarded a PhD in control theory and systems biology from the University of Stavanger in 2020. Daniel has been heavily engaged with interdisciplinary research, in areas ranging from control engineering and signal processing to systems biology and cancer metabolism.

Karolina Di Remigio Eikås, Ph.D., is a Scientist at the Norwegian Defence Research Establishment (FFI), where she has worked since 2024. Her research is focusing on modeling and simulation of multi-domain operations. Karolina has a PhD in theoretical chemistry from UiT – The Arctic University of Norway in 2022.

Requirements for Simulation of the Future Operating Environment and Multi-Domain Operations

Per-Idar Evensen, Even Soltvedt Hvinden, Helene Rødal Holhjem,
Daniel Myklatun Tveit, Karolina Di Remigio Eikås
Norwegian Defence Research Establishment (FFI)
Kjeller, Norway
per-idar.evensen@ffi.no, even-soltvedt.hvinden@ffi.no, helene-rodal.holhjem@ffi.no,
daniel-myklatun.tveit@ffi.no, karolina-di-remigio.eikas@ffi.no

INTRODUCTION

The future operating environment is expected to become increasingly complex, lethal, and ambiguous. The operational tempo in high-intensity operations is expected to increase, and effects will be increasingly cross-domain and contemporaneous. An essential question is: How can our forces conduct successful military operations in the envisioned future operating environment?

The proposed solution is *multi-domain operations* (MDO). MDO is an operational concept where the underlying idea is seamless integration of capabilities and activities in all the operational domains (land, maritime, air, space, and cyberspace), to present the enemy with multiple simultaneous dilemmas and achieve overwhelming superiority in time and space on the battlefield. MDO will, however, be inherently much more complex to execute than current operations of the same scale, due to a higher diversity of combat elements and capabilities (from all operational domains), higher requirements for synchronization of capabilities, activities and actions, and higher requirements for operational tempo.

Experimentation and analysis are key enablers for concept development and provide the ability to iteratively explore, test, refine, and validate concepts (NATO ACT, 2021). Modeling and simulation (M&S) and wargaming will be essential in experimentation with, and further development and detailing of, the MDO concept. However, M&S of the future operating environment and MDO will also be correspondingly more complex. In addition, very few, if any, of the simulation tools currently available can represent combat elements and capabilities in all operational domains at a sufficient and balanced level of fidelity throughout the combat model.

In this paper we first outline the background for the work described in this paper. Then, we give a summary of how the future operating environment is envisioned to be like in a 2025–2045 perspective and what technologies are expected to dominate on the battlefield, based on recent literature. Moreover, we provide a description of the concept of MDO, including definitions, historical origin, characteristics, and challenges. Finally, we outline and discuss a set of overall requirements for simulation of the future operating environment and MDO for concept development, experimentation, and analysis.

BACKGROUND

Combat simulations in various forms for concept development, experimentation, and analysis have been carried out at the Norwegian Defence Research Establishment (FFI) for decades. Simulation experiments are often used to test out new concepts, or to assess and compare the performance and combat effectiveness of different combat systems, for example weapon systems, combat structures, or force structure elements (Martinussen et al., 2008; Hoff et al., 2012; 2013). Our general approach for using simulations to assess and compare the relative combat effectiveness of different combat systems has been described in Evensen et al. (2022a) and Evensen et al. (2022b).

Our simulation experiments can be categorized as *discovery experiments* or *hypothesis testing experiments*. *Discovery experiments* involve introducing novel systems, concepts, organizational structures, technologies, or other elements to a setting where their use can be observed and catalogued (Alberts & Hayes, 2002). *Hypothesis testing experiments* are used to advance knowledge by seeking to falsify specific hypotheses or discover their limiting conditions (Alberts & Hayes, 2002).

There are mainly two approaches for conducting combat simulations: using fully automated *closed-loop simulations* (without any human interaction) or using *human-in-the-loop (HITL) simulations* (with varying degrees of human interaction). *Closed-loop simulations* can be run faster than real-time and thus repeated many times to get a statistical distribution of the outcomes, but they give a less realistic representation of the human aspects of combat. *HITL simulations* must be run in real-time and can therefore only be repeated a few times, but they give a more realistic representation of the human aspects of combat. HITL simulations are mainly associated with *virtual* simulations in the live, virtual, and constructive (LVC) taxonomy, but *constructive* simulations may also require a certain degree of human interaction, for example to control semi-automated forces (SAF). Generally, we use *virtual* simulations in experiments where human system operators are essential, for example to experiment with technologies or concepts that directly affect human performance or how humans operate at the technical level. In our discovery experiments, which are often focused on trying out new technologies and new ways of operating, we use HITL simulations. In our hypothesis testing experiments, which are often focused on comparing the performance and effectiveness of different combat structures and different ways of operating, we have also mainly used HITL simulation, but in the future, we plan to adopt the hybrid approach described by Willis et al. (2023) and use both HITL and closed-loop simulations.

At FFI, a lot of simulations are conducted at the technical/sub-tactical level in research projects supporting the development, procurement, or use of specific systems/materiel (combat aircraft, air defense, etc.). The results from these simulations are used to calibrate simulations at the tactical level. Furthermore, the results from simulations at the tactical level are used to calibrate simulations at the operational level. Simulations at the operational level may also reveal new research questions that need to be analyzed in more detailed simulations at the tactical level. This is illustrated in Figure 1.

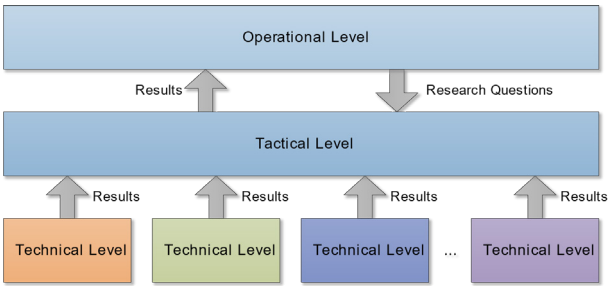

Figure 1. Different Levels of Simulation.

There is now a focus on MDO, and consequently we need to establish a capability for simulation of MDO at FFI. We are therefore conducting a study that has three phases:

1. Envisage/describe the future operating environment and MDO.
2. Define requirements for a synthetic environment for simulation of the future operating environment and MDO at the tactical/engagement level and the operational level.
3. Evaluate available simulation tools based on the requirements.

This paper describes the results from the first two phases of this study. The third and last phase is future work.

THE FUTURE OPERATING ENVIRONMENT AND MULTI-DOMAIN OPERATIONS

In this section, we first look at the five operational domains. Then, we look at how the future operating environment is envisioned to be like in the next twenty years. Finally, we look at the concept of MDO, including definitions, historical origin, characteristics, and challenges.

Operational Domains

There is no unified, agreed upon definition of what an *operational domain* is. The North Atlantic Treaty Organization (NATO) defines an operational domain as "[a] specified sphere of capabilities and activities that can be applied within an engagement space" (NSO, n.d.). In the *U.S. Army Field Manual 3.0 – Operations* (Department of the Army, 2022), an operational domain is defined as "a physically defined portion of an operational environment requiring a unique set of warfighting capabilities and skills". Another frequently used definition has been proposed by MDO expert Jeffrey M. Reilly, who defines an operational domain as a "[c]ritical macro manoeuvre space whose access or control is vital to the freedom of action and superiority required by the mission" (Donnelly & Farley, 2019). How to maneuver in a domain is often a unique, defining feature that separates the domains from each other (Donnelly & Farley, 2019). NATO defines five operational domains: the *land domain*, the *maritime domain*, the *air domain*, the *space domain*, and the *cyberspace domain* (NSO, 2022). The land, maritime, air, and space domains are defined by their location and

physical characteristics, whereas the cyberspace domain exists in a human-made web of networks that extend throughout and connect the other domains. The operational domains are useful as a mental framework for understanding the operating environment and planning operations. It is through the operational domains that military and non-military organizations integrate their capabilities (NSO, 2022).

The Future Operating Environment 2025–2045

An *operating* or *operational environment* can be defined as "[a] composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander" (NSO, n.d.). Operating environments are the surroundings or settings for military operations (UK MOD, 2020). Predicting how the future operating environment will be like is a difficult task. However, there are several recent reports, for example UK MOD (2014), TRADOC (2019), AFC (2021), and NATO STO (2023), that attempt to describe the characteristics of plausible future operating environments based on current trends. In this subsection, we summarize how the future operating environment is expected to be like in a 2025–2045 perspective and what technologies are expected to dominate on the battlefield.

Overall, the future operating environment is expected to become increasingly complex, lethal, and ambiguous (UK MOD, 2014). Potential adversaries will adopt hybrid strategies that blur the distinction between war and peace and often operate below the threshold of warfare using proxy forces, criminal elements, or terrorists (Sullivan et al., 2017; TRADOC, 2019; AFC, 2021). The operational tempo in high-intensity operations is expected to increase, and effects will be delivered in all operational domains (Sullivan et al., 2017; TRADOC, 2018). The space and cyberspace domains will become increasingly important. Furthermore, because of population growth and increased urbanization, the operating environment can be expected to include dense urban environments (Sullivan et al., 2017; TRADOC, 2018; 2019).

In the future operating environment, it is expected that more and better sensors (in all domains), connected through sensor networks, combined with artificial intelligence (AI) for data analysis, may enable very good situational awareness, in near real time. Sensor proliferation will make it increasingly difficult for military forces to stay hidden, and surprising an adversary may be more difficult (TRADOC, 2019; UK MOD, 2020). The realized situational awareness will depend on the balance between own capabilities and opponent countermeasures.

Potential adversaries are expected to make extensive use of sophisticated anti-access (A2) and area denial (AD) capabilities. This will largely deny access to, and freedom of movement within, operational areas (UK MOD, 2014; Sullivan et al., 2017; TRADOC, 2019).

Technology will be essential in the future operating environment and a key driver of military change (UK MOD, 2014; TRADOC, 2019; AFC, 2021; NATO STO, 2023). Overall, technological developments are expected to be increasingly *intelligent*, *interconnected*, *decentralized*, and *digital*, and this, in turn, will lead to military capabilities that are increasingly *autonomous*, *networked*, *multi-domain*, and *precise* (NATO STO, 2023). It is also expected that increased proliferation of technology will make gaining and sustaining technological advantage increasingly challenging (UK MOD, 2014; NATO STO, 2023).

The following technologies are anticipated to be most important for the future operating environment in a 2025–2045 perspective (UK MOD, 2014; TRADOC, 2019; UK MOD, 2020; AFC, 2021; NATO STO, 2023):

- **Artificial intelligence (AI):** AI will probably be the most important technology the next two decades, and it will play a significant role in the future operating environment. Important military application areas for AI are autonomous systems, data analysis, decision support, and information operations.
- **Autonomous and unmanned vehicles:** The use of autonomous and unmanned vehicles, across multiple domains, is expected to increase substantially in the future operating environment. Autonomous and unmanned vehicles have historically been used to do the dull, dirty, and dangerous tasks. Examples of more advanced applications for autonomous and unmanned vehicles in military operations, that we will see in the future, are manned-unmanned teaming (MUM-T) and swarms of small, low-cost, self-organizing autonomous vehicles used both offensively and defensively.
- **Quantum technologies:** Quantum technologies exploit quantum physics and associated phenomena, like quantum entanglement and superposition, and are anticipated to provide significant technological

advancements in the coming decades. For example, quantum computing is expected to provide vast increasements in data processing capabilities, and quantum sensing is expected to provide more precise, ultra-sensitive sensors.

- **Sensor technology:** Advances in sensor technologies (for example within quantum sensing) are expected to create better, smaller, and cheaper passive and active sensors that are networked and distributed across all environments, including space.
- **Information technology (IT):** IT will continue to improve, providing a greater degree of connectivity and enabling decentralization. As a result, the cyberspace domain will become increasingly important in the future operating environment.
- **Bio and human enhancement technologies (BHET):** BHET are expected to mature and become available over the next twenty years.
- **Additive manufacturing:** Additive manufacturing will enable on site production and repair of military materiel and thus make the logistics chain lighter.
- **Hypersonic technologies:** Missiles, aircraft, and drones capable of flying at hypersonic speeds (i.e., five times the speed of sound or greater) are expected to be important capabilities in the future operating environment.
- **Advanced long-range precision fires:** The availability, range, speed, and accuracy for precision guided munitions are expected to increase.
- **Directed energy weapons:** Directed energy weapons, like laser weapons, microwave weapons, and electromagnetic pulse (EMP) weapons, have matured and are expected to be even more widely used over the next few years.
- **Cyber and electronic warfare tools:** The cyberspace domain will become increasingly important in the future, and cyber and electronic warfare tools will be ubiquitous. Offensive and defensive cyber and electronic warfare capabilities will become increasingly important in future operations.
- **Anti-satellite weapons:** The space domain will become increasingly important in the future, and ground- or space-based anti-satellite weapons are expected to be fielded.

Almost every new technology is linked to, and intersects with, other new technologies, and disruptive effects will often occur through technology convergence driven by combinations of new technologies (TRADOC, 2019; NATO STO, 2023). Examples of synergies and combinations that have the potential to highly influence the development of future military capabilities are IT, AI, and autonomous and unmanned vehicles; IT, AI, and BHET; sensor technology, quantum technologies, and AI; and IT and quantum technologies.

Multi-Domain Operations

An essential question is: How can we conduct successful military operations in the envisioned future operating environment described in the previous subsection? The proposed solution is *multi-domain operations* (MDO). MDO is an operational concept where the underlying idea is seamless integration of capabilities and activities in all the operational domains (land, maritime, air, space, and cyberspace), to present the enemy with multiple simultaneous dilemmas and achieve overwhelming superiority in time and space on the battlefield. NATO's definition of MDO is: "The orchestration of military activities, across all operational domains and environments, synchronized with non-military activities, to enable the Alliance to create converging effects at the speed of relevance" (NSO, n.d.). The concept of MDO can be seen as a natural evolution of joint operations (NSO, 2022). MDO has increased emphasis on the space and cyberspace domain. MDO is also more focused on seamless integration and synchronization of capabilities from all domains at all levels of warfare and especially at the tactical/engagement level, increased operational tempo, and synchronization with non-military activities. Figure 2 illustrates the concept of MDO.

The initial concept for MDO was developed by U.S. Army (TRADOC, 2018). The concept draws from previous U.S. Army operational concepts, including AirLand Battle, Full Spectrum Operations, and Unified Land Operations (Department of the Army, 2022). From the perspective of military theory, MDO has evolved from linear operations, non-linear operations, and strategic paralysis theory (Kasubaski, 2019). U.S. Army's definition of MDO is: "Operations conducted across multiple domains and contested spaces to overcome an adversary's (or enemy's) strengths by presenting them with several operational and/or tactical dilemmas through the combined application of calibrated force posture; employment of multi-domain formations; and convergence of capabilities across domains, environments, and functions in time and spaces to achieve operational and tactical objectives" (TRADOC, 2018).

Development of the MDO concept was initiated in November 2011 when General Martin E. Dempsey, chairman of the U.S. Joint Chiefs of Staff, asked the Military Education Coordination Council the prophetic question, "What's after joint?" (Reilly, 2016). "General Dempsey's inquiry was spurred by the fact that historical approaches to achieving superiority in the air, land, and sea domains may no longer be valid. The principal factor driving this phenomenon is a global proliferation of advanced information technology" (Reilly, 2016). The MDO concept has now been embraced by NATO and its nations.

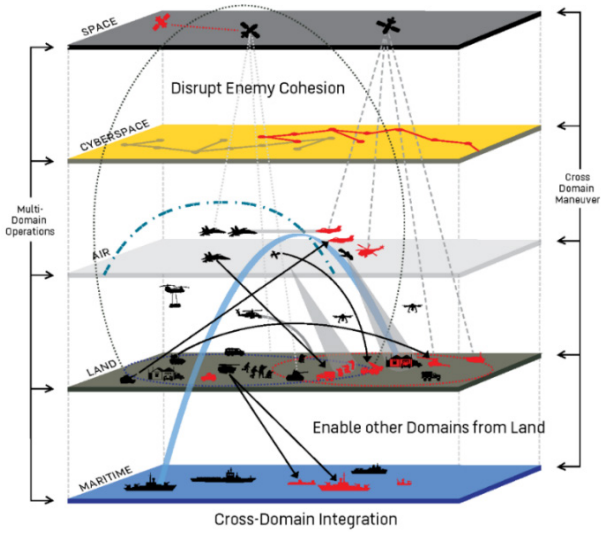

Figure 2. The Concept of Multi-Domain Operations (MDO) (U.S. Army, 2020).

The MDO concept is based on a strategic environment with a competition continuum with three categories of strategic relationships: *cooperation*, *competition below armed conflict*, and *armed conflict* (Department of the Army, 2022). It seeks to solve the problem of multiple layers of *stand-off*[1] in all domains (e.g., ballistic missiles, cruise missiles, information and cyber warfare, unconventional warfare, and long-range fires), employed by strategic competitors like Russia and China to disrupt the coherence in operations by U.S. and allied forces (TRADOC, 2018). More specifically, the MDO concept seeks to solve the following five operational problems (TRADOC, 2018):

1. How does the Joint Force *compete* to enable the defeat of an adversary's operations to destabilize the region, deter the escalation of violence, and, should violence escalate, enable a rapid transition to armed conflict?
2. How does the Joint Force *penetrate* enemy A2 and AD systems throughout the depth of the support areas to enable strategic and operational maneuver?
3. How does the Joint Force *dis-integrate* enemy A2 and AD systems in the deep areas to enable operational and tactical maneuver?
4. How does the Joint Force *exploit* the resulting freedom of maneuver to achieve operational and strategic objectives through the defeat of the enemy in the close and deep maneuver areas?
5. How does the Joint Force *re-compete* to consolidate gains and produce sustainable outcomes, set conditions for long-term deterrence, and adapt to the new security environment?

The solution to these problems is addressed through three tenets of MDO (TRADOC, 2018):

1. *Calibrated force posture*: the combination of capacity, capability, position, and the ability to maneuver across strategic distances.
2. *Multi-domain formations*: the capacity, capability, and endurance necessary to operate across multiple domains in contested spaces against a near-peer adversary.
3. *Convergence*: the rapid and continuous integration of capabilities in all domains across time and space to overmatch the enemy.

The three tenets are underpinned by mission command and disciplined initiative at all warfighting echelons (TRADOC, 2018). They are mutually reinforcing and common to all MDO, but how they are realized will vary by echelon and depend upon the specific operational situation (TRADOC, 2018).

MDO is an operational concept. Going forward, this concept must be further developed, tested, and validated through experimentation. M&S and wargaming will be essential in this work. A successful concept, that demonstrates significant credible improvement, will ultimately be transitioned into operational doctrine (NSO, 2022).

[1] *Stand-off* is the political, temporal, spatial, and functional separation that enables freedom of action in any, some, or all domains, the electromagnetic spectrum, and the information environment to achieve strategic and/or operational objectives before an adversary can adequately respond (Joint Chiefs of Staff, 2019).

The concept of MDO is quite ambitious, and there are several challenges that need to be resolved to conduct effective MDO. MDO requires the synchronizations of capabilities, activities, and actions that literally range from the speed of light to walking pace (NSO, 2022). A key challenge is effective integration and synchronization of kinetic actions with actions in the cyberspace domain and information dimension (Gady & Stronell, 2020).

MDO also requires highly trained commanders and personnel that can think, plan, and act across all domains and environments. Moreover, effective multi-domain command and control (C2) requires a resilient technical architecture, flexible command relationships, and multi-domain control measures (TRADOC, 2018).

Critical contributions by NATO nations and partners to MDO will include supporting the calibrated force posture of Alliance forces, expertise to effectively compete below the threshold of armed conflict, supporting the development of critical capabilities that enable long-range precision fires, and providing expertise and capabilities in the conflict phase (Watling & Roper, 2019). Not all allies require the same level of sophisticated equipment to contribute to MDO, but critical challenges that need to be addressed are shared situational awareness, coordinating synchronic operations, and training for conducting MDO (Watling & Roper, 2019).

Interoperability across NATO nations and partners, services, and agencies is a key element to executing MDO (TRADOC, 2018). A main barrier to interoperability is "the lack of a common language across the alliance to describe the multi-domain environment, and to communicate changes in that environment" (Watling & Roper, 2019).

There are also concerns regarding the maturity of the technology which effective MDO will rely upon, for example a high level of assured communications connectivity (Ellison & Sweijs, 2023). Furthermore, there are real concerns about whether MDO will mature into a fully functional operational concept (Ellison & Sweijs, 2024).

SIMULATION OF MULTI-DOMAIN OPERATIONS

M&S and wargaming will be essential in further development of, and experimentation with, the MDO concept. However, very few, if any, of the simulation tools currently available can represent combat elements, capabilities, and effects in all operational domains at a sufficient and balanced level of fidelity throughout the combat model. In this section we discuss some of the challenges with M&S of MDO and how suitable today's simulation tools are for simulation of MDO.

Future MDO will be inherently much more complex to execute than current operations of the same scale, due to a higher diversity of combat elements and capabilities from all operational domains, higher requirements for synchronization of capabilities, activities and actions, and higher requirements for operational tempo. In the same way, M&S of MDO will also be much more complex.

Most military simulation tools are primarily developed to be used for training, but they can also be used for experimentation and analysis. Furthermore, their development has often mainly been financed by one of the traditional military services (Army, Navy, or Air Force). Most of the simulation tools available today have therefore been developed to primarily represent combat in one of the traditional operational domains. Elements from the other two traditional domains may also be represented, but with a lower fidelity. Very few simulation tools include models of capabilities in the space and cyberspace domains.

With the current focus on MDO, and the need for further developing and experimenting with this concept, there is now a need for simulation tools that represent combat elements, capabilities, and effects in all operational domains. There will gradually also be a greater need for simulation tools for training of MDO. The development of simulation tools to support simulation of MDO will of course take time and require funding, but in the future, combat simulation tools above the technical/sub-tactical level that are not able to represent combat elements and activities across all operational domains risk becoming irrelevant.

An initiative addressing this need is the NATO Next Generation M&S, which is envisioned to be a data-centric, web-based, modular, single synthetic environment developed to support NATO commands and nations with wargaming, experimentation, planning, and training in a multi-domain operating environment. This capability will, however, not become available before 2030.

REQUIREMENTS FOR SYNTHETIC ENVIRONMENT

When using simulation for experimentation and analysis, the specific requirements for the synthetic environment will ultimately depend on the objective of the simulation, for example to answer a specific research question. Nevertheless, the overall requirement is that we need a holistic synthetic environment as a basis for experimenting with, and analyzing, combat across all operational domains in an operating environment five to twenty years into the future. Furthermore, we envisage that we need to provide insight into both detailed research questions at the tactical/engagement level and more overarching research questions at the operational level. In this section, we therefore first describe typical use cases for experimentation at the tactical/engagement level and at the operational level and then outline a set of general requirements for simulation of MDO in a future operating environment at both levels of simulation. A synthetic environment that meets most of these requirements will serve as a starting point that can more easily be adapted for conducting tailored simulation experiments to get insight into specific research questions related to the future operating environment and MDO. The synthetic environment will be exclusively used to simulate the actual combat phases of MDO. It will not be used for simulations at the strategic level.

Use Cases

Tactical/Engagement Level

Typical use cases for simulations at the tactical/engagement level include experimentation with C2 solutions, synchronization of effects from multiple domains, new technologies, tactics, techniques, and procedures (TTP), and different combat structures. At this level we typically use constructive simulations with SAF controlled by human operators/role-players, occasionally together with some virtual entities, like combat aircraft and other weapon platforms. The virtual entities will typically be controlled by system operators in externally connected simulators. For hypothesis testing experiments, we also want to use constructive closed-loop simulations.

Operational Level

Typical use cases for simulations at the operational level include experimentation with C2 solutions, resource allocation between parallel missions, coordination and synchronization of activities, handling increased complexity, new technologies, operational concepts, and different force structure elements. At this level we typically use constructive simulations with SAF controlled by human operators, but for hypothesis testing experiments, we also want to use constructive closed-loop simulations.

General Requirements

In this subsection we outline FFI's general requirements for a synthetic environment for simulation of the future operating environment and MDO at the tactical and operational levels in the Norwegian theater.

Software Architecture

For us it is preferable to use the same simulation system for simulations at the tactical/engagement level and operational level, because acquiring, administering, and maintaining only one main simulation system will be cheaper and require fewer human resources. For the same reasons, and since the interactions between the domains will be much more extensive in MDO, we also prefer to use one single simulation system that supports all domains, instead of connecting two or more simulation systems that only support a subset of the five domains. Moreover, it will be an advantage if the simulation system has a software architecture based on modular microservices since this will provide increased scalability and flexibility for future demands.

Aggregation Level

With today's computing power it is feasible to simulate operations with tens of thousands of military platforms using entity-level models. Regardless, it would be problematic to use aggregate-level models to conduct detailed simulations of MDO, due to the higher flexibility in more ad hoc composition of different combat elements. Furthermore, in a future operating environment where it will be more difficult for units to stay undetected, forces will probably need to operate more dispersed to avoid forming clusters of targets for the enemy. It would also be difficult to calibrate aggregate-level models to represent new technologies and new concepts in a future operating environment, due to the lack of attrition data from real operations. Hence, our requirements for the synthetic environment are:

- It *must* represent individual vehicles (ground vehicles, aircraft, ships, etc.) and individual dismounted soldiers.
- Larger entities *must* be able to transport (and deploy) smaller entities (e.g., ground vehicles may transport UAVs, ships may transport helicopters, and vehicles may transport dismounted soldiers).

Number of Entities
The required number of entities are given by our operational level use cases, that is the expected size and intensity of MDO in the Norwegian theater. In the most demanding scenario, the sum of Norwegian and allied forces, a symmetric adversary, and civilian entities implies a minimum requirement of approximately ten thousand entities:

- The simulation *must* be able to represent a minimum of ten thousand entities simultaneously. The maximum number of entities that can be simulated will, however, always also depend on the capacity of the computer system running the simulation.

Resolution and Fidelity
There are two main approaches for modeling sensing, effects, and communication: (1) using probability-based models or (2) using physics-based models. Some simulation systems use a combination of both approaches. The physics-based approach will usually have a higher fidelity, but at the cost of requiring more computing power to simulate the same number of entities. We have a preference towards physics-based models because it is usually easier to find data for configuration and calibration of such models, but probability-based models at the entity-level are also acceptable.

Valid inference requires that resolution and fidelity are both (1) *sufficient* to represent the difference in performance between combat systems and (2) *balanced* so the relative performance of combat systems is not an artifact of model implementations tailored for a specific domain, but rather the technical or technological performance of the combat systems. Consequently, MDO simulations for experimentation and analysis impose strict requirements on simulation models to account for interactions across all domains, making the implementation of high-fidelity MDO simulation models more comprehensive and time-consuming. For an MDO simulation to meet the requirement of having a sufficient and balanced level of fidelity throughout the combat model, it is important that subject matter experts (SMEs) and role-players from the five domains can contribute to the MDO with the capabilities and effects they want and have roughly the same perception of the fidelity of the representation of the capabilities and effects in their respective domains.

Synthetic Natural Environment
A *synthetic natural environment* (SNE) represents the physical world in which the simulated combat units operate and usually includes the terrain with seas, lakes, rivers, and vegetation and human-built structures like roads, runways, bridges, and buildings. Our most important requirements for the SNE are:

- It *must* use a spherical whole earth model. This is especially important for simulation of capabilities like satellites, aircraft, missiles, long-range fires, and long-range sensors, which will be important for the future operating environment and MDO.
- It *must* be able to represent areas of interest with a resolution of ten meters between the elevation points (Digital Terrain Elevation Data – DTED Level 3), or better. Norway has steep and hilly terrain that will affect the movement of forces and the coverage of sensors and communication systems, so it is important with high terrain resolution to have a good representation of the effects terrain can have on MDO. For example, we have seen that lower terrain resolution makes cover and concealment difficult, and this systematically favors long-range, direct fire weapon systems (Evensen & Bentsen, 2016).
- It *must* be able to represent different land-cover materials (soil, mud, gravel, rock, grass, asphalt, snow, ice, etc.) with different trafficability. This requirement is important for realistic movement of land forces.
- It *must* be able to represent vegetation (trees, bushes, etc.) and bodies of water (oceans, lakes, rivers, etc.).
- It *must* be able to represent static human-made structures (roads, runways, bridges, buildings, etc.) and support generation of dense urban environments. Dense urban environments are expected to be an important part of the future operating environment.
- It *must* be able to represent an underwater environment with bathymetric data at DTED Level 1, or better. A realistic representation of the underwater environment is necessary to simulate the propagation of underwater sound, and hence the validity of underwater sensor and signature models.

- It *must* be able to represent weather (fog, clouds, wind and sea state, and precipitation) and climate. The northern part of Norway has an arctic climate where the weather can be severe. This can affect the movement of forces and the effectiveness of sensors, and thus seriously impact the effectiveness of MDO.

Capabilities and Effects in All Domains

For simulation of MDO it is crucial with representation of capabilities and effects in the three traditional domains (land, maritime, and air) at a balanced level of fidelity, in addition to representation of capabilities and effects in the cyber and space domains. A balanced level of fidelity is important to reduce the risk of introducing systematic biases in the simulation. More specifically, our most important requirements for capabilities and effects are:

- The synthetic environment *must* include simulation models of all main military platform types from the three traditional domains. This includes soldiers, vehicles (wheeled and tracked), ships/vessels, submarines, aircraft (fixed wing and rotary wing), and unmanned systems (UGVs, USVs, UUVs, and UAVs). This also includes different types of weapons/effectors and effects (kinetic and non-kinetic), countermeasures and protection systems, decoys, and passive and active sensors (optical, electromagnetic, thermal, and acoustic). Furthermore, this includes hypersonic missiles and aircraft, drone swarms, and directed energy weapons (laser, microwave, and EMP), which are capabilities that are expected to be important for the future operating environment.
- The synthetic environment *must* include simulation models of satellites and ground- or space-based anti-satellite weapons. Satellites for communication and sensing will be important capabilities in the future operating environment, and the destruction of these capabilities could seriously impact the effectiveness of MDO.
- The synthetic environment *must* include simulation models of communication systems and infrastructure, communication and data transfer, and the most important capabilities and effects in the cyberspace domain for conducting electromagnetic warfare (EW) and cyberspace operations (CO). Important effects for EW and CO include jamming, denial of service, spoofing, deception, targeting, espionage, sabotage, disruption, and data exfiltration (Bates et al., 2023). Effective MDO will rely upon a high level of assured communication for synchronization of capabilities and effects, but communications can be disrupted, and platforms emitting electromagnetic waves can be more easily detected. These effects need to be represented in the synthetic environment.
- The synthetic environment *must* include basic simulation models of C2 units (nodes and headquarters), intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) units (sensors and facilities), air defense units (sensors and effectors), combat engineering units (including obstacles and mines), logistics and supply units (on site production, transportation, and facilities), and medical units (in-field support, transportation, and facilities).
- The synthetic environment *must* support a flexible C2 structure, which enables representation of a cross-domain kill web of sensors, C2 nodes, and effectors, where combat elements from different domains can be transferred between commanders and put together for different tasks and missions during runtime. This requirement is important for simulation of MDO at the operational level.

Behavior Models

Behavior models represent the behavior of humans and unmanned systems and are important to reduce the number of human operators and avoid that the operators must spend a lot of time micromanaging the entities. Human behaviors are complex and very challenging to model, and the increased complexity of MDO will entail even more complex behavior models with more factors to consider, for example synchronization of effects and threats from all domains. Our most important requirements for behavior models are:

- The synthetic environment *must* include basic behavior models for the most important tasks or missions, such as move to location, attack enemy unit/area, including delivery of effects on a target at a specified time, defend/protect area, and suppress enemy unit, for different types of combat entities in all domains. Behavior models that can synchronize and converge effects are important for simulation of MDO.
- The synthetic environment *must* include basic behavior models for pattern of life for civilian entities. Dense and crowded urban environments are expected to be an important part of the future operating environment.
- The synthetic environment *should* include AI-based behavior models where the entities are able to make intelligent decisions based on their perception of the environment to reach or adjust their goals.

User Interface for Human-in-the-Loop Simulations
The purpose of the user interface (UI) for the operators/role-players in a HITL simulation, is to provide a common operational picture based on information shared by sensor in the simulated environment and other relevant information created and shared by the operators. Furthermore, the operators must be able to assign orders to their forces. HITL simulations for MDO will be executed with military SMEs as operators. This means that the UI must be easy to use. Our most relevant requirements for the synthetic environment regarding the operator UI:

- It *must* have an easy-to-use UI for commanding and controlling forces in all domains.
- It *must* have tools for planning operations. This includes assigning orders to forces visualized with tactical graphics and a synchronization matrix for synchronizing capabilities, activities, and actions in MDO.
- It *should* have functionality for tailoring the UI for specific operator roles.

Customization
The synthetic environment for simulation of the future operating environment and MDO must be able to represent combat across all operational domains in an operating environment five to twenty years into the future. We currently do not know exactly what future platform types, effectors, sensors, and behavior models we want to experiment with going forward. Hence, the most relevant requirements for customization of the synthetic environment are:

- It *must* support customization of entities, weapons, sensors, and behavior models.
- It *must* have an application programming interface (API) for developing own models and extensions.

Interoperability
Depending on the purpose of the simulation experiment it might be necessary to connect the synthetic environment for MDO to other simulation tools (e.g., virtual simulators) and/or C2 systems. This requires interoperability between the simulation systems and C2 systems, and leads to the following interoperability requirements for the synthetic environment:

- It *must* support existing interoperability standards for distributed simulations such as Distributed Interactive Simulation (DIS) and/or High Level Architecture (HLA).
- *It should* be interoperable with C2 systems.

Data Collection
Valid inference from a simulation experiment will generally require a detailed statistical analysis of the data. Moreover, a simulation experiment can be facilitated by instructive real-time visualizations of key variables. When simulating MDO, the high number of entities combine with cross-domain dependencies to create both large amounts of data and complex causal relationships. Hence, we require that the synthetic environment features the following data collection capabilities:

- It *must* support logging of relevant data, including events, actions, effects, and entity state variables, for example, orders, position, speed, heading, data links, and sensor detections and tracks.
- It *should* support playback capabilities of logged data for after-action review (AAR).
- It *should* support real-time visualizations of combat performance and effectiveness data, e.g. kill matrices, loss-exchange ratios, and supply expenditures.

Discussion

The core idea of MDO is the seamless integration of effects across domains. A valid simulation of MDO therefore poses two requirements that are less prominent in domain-specific simulations:

1. A valid MDO simulation requires a *simultaneous high minimal level of size and fidelity*. The expected proliferation of cross-domain effects requires that all domains are represented simultaneously, increasing the effective size of the battlespace and the number of interacting entities. At the same time, we require that the interaction between entities and their operating environment is valid, placing a high lower bound on the necessary resolution and fidelity of each model. In contrast, for domain-specific simulations it is generally possible to limit the size or fidelity of the simulation while maintaining validity.

2. We expect that a binding restriction on the integration of cross-domain effects will be the presence and functioning of robust and high-performance command, control, and communication (C3) networks. Hence, defending own C3 networks, and degrading enemy C3 networks, are expected to be an important component of MDO. A valid MDO simulation requires an *explicit model of C3 networks*.

The implication is that, all else equal, M&S of MDO will require a simulation model of substantial size and complexity when compared to a domain-specific simulation model. We do not expect a single simulation model to fully meet all our stated requirements. The evolution of the MDO concept is subject to considerable uncertainty, and we must expect that the desired properties of the simulation model evolve. The high minimum size and complexity of the simulation model, combined with the uncertainty over future use-cases, imply that the salient trade-offs between requirements are uncertain. In turn, uncertainty concerning the trade-offs between requirements emphasize the value of an agile testing and evaluation strategy. We expect that developing our requirements through repeated tests of parsimonious scenarios will be more productive than attempting detailed *ex-ante* specification.

FURTHER WORK

We will use the requirements outlined in this paper to evaluate available simulation tools. Moreover, we will test the most promising candidates more thoroughly and hopefully end up with a candidate that is sufficient for our needs.

SUMMARY AND CONCLUSION

In this paper, we have given a summary of how the future operating environment is envisioned to be like in a 2025–2045 perspective and a description of the concept of MDO. Moreover, we have discussed and outlined a set of overall requirements for a synthetic environment for simulation of the future operating environment and MDO, at the tactical and operational levels, for concept development, experimentation, and analysis. We will use these requirements to evaluate available simulation tools and finally test the most promising candidates more thoroughly.

Our preference is to have one simulation system that supports all domains, instead of connecting two or more simulation systems that only support a subset of the five domains. However, a single simulation system that meets all our requirements may not yet exist. Nevertheless, we need to establish a capability for simulation of MDO at FFI as soon as possible, so we may have to go for an interim solution that meets as many of the most important requirements as possible.

ACKNOWLEDGEMENTS

We would like to thank our I/ITSEC Birddog Nick Giannias for his helpful comments and suggestions during the process of developing this paper.

REFERENCES

Alberts, D.S & Hayes, R.E. (2002). *Code of Best Practice for Experimentation*, The Command and Control Research Program (CCRP) Publication Series.

Bates, C., Cox, J., Heidelbaugh, C., Ruth, J., & Friest, T. (2023). Contextualizing Cyberspace Electromagnetic Activities (CEMA) in Multi-Domain Operations (MDO) Through Playbooks, *Proceedings of the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC) 2023*, Paper No. 23179.

Department of the Army. (2022). *Operations*. Field Manual No. 3-0.

Donnelly, J. & Farley, J. (2019). Defining the 'Domain' in Multi-Domain. *Joint Air & Space Power Conference 2019 Read Ahead*.

Ellison, D & Sweijs, T. (2023). *Breaking Patterns: Multi-Domain Operations and Contemporary Warfare*. The Hague Centre for Strategic Studies (HCSS).

Ellison, D & Sweijs, T. (2024). *Empty Promises? A Year Inside the World of Multi-Domain Operations*. War on the Rocks. Retrieved April 17, 2024, from https://warontherocks.com/2024/01/empty-promises-a-year-inside-the-world-of-multi-domain-operations.

Evensen, P.-I. & Bentsen, D.H. (2016). *Simulation of land force operations – a survey of methods and tools*, Norwegian Defence Research Establishment (FFI), FFI report 2015/01579.

Evensen, P.-I., Halsør, M. & Bentsen, D.H. (2022a). Estimating Relative Combat Effectiveness Using Simulations. *Proceedings of the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC) 2022*, Paper No. 22137.

Evensen, P.-I., Halsør, M., Hoppe, U.-P. & Bentsen, D.H. (2022b). *Measuring combat effectiveness*. Norwegian Defence Research Establishment (FFI), FFI report 21/02310.

Gady, F.-S. & Stronell, A. (2020). Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030. In *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Ertan, A., Floyd, K., Pernik, P. & Stevens, T. (edited by). NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

Hoff, E.Ø., Evensen, P.-I., Holhjem, H.R., Øyan, I.B. & Nygård, H.K. (2012). Simulation in Support of Army Structure Analysis. *Proceedings of the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC) 2012*, Paper No. 12088.

Hoff, E.Ø., Evensen, P.-I., Holhjem, H.R., Øyan, I.B. & Nygård, H.K. (2013). Interactive Simulation to Support the Transition of Forces. *Proceedings of the NATO Modelling and Simulation Group (NMSG) Annual Symposium 2013 (STO-MP-MSG-111)*, Paper No. 6.

Joint Chiefs of Staff. (2019). *Joint Land Operations*. Joint Publication 3-31.

Kasubaski, B.C. (2019). Exploring the Foundation of Multi-Domain Operations. *Small Wars Journal (SWJ)*.

Martinussen, S.E., Tansem, I., Evensen, P.-I.., Rødal, H. & Bore, I. (2008). Simulation in Support of Defence Structure Analysis. *Proceedings of the NATO Modelling and Simulation Group (NMSG) Annual Symposium 2008 (RTO-MP-MSG-060)*, Paper No 22.

North Atlantic Treaty Organization (NATO) Allied Command Transformation (ACT). (2021). *NATO CD&E Handbook – A Concept Developer's Toolbox*. Version 2.10.

North Atlantic Treaty Organization (NATO) Science & Technology Organization (STO). (2023). *Science & Technology Trends 2023–2043, Volume 1: Overview*.

North Atlantic Treaty Organization (NATO) Standardization Office (NSO). (n.d.). NATOTerm – The Official NATO Terminology Database. Retrieved April 16, 2024, from https://nso.nato.int/natoterm.

North Atlantic Treaty Organization (NATO) Standardization Office (NSO). (2022). *Allied Joint Doctrine*. Allied Joint Publication (AJP)-01, Edition F, Version 1.

Reilly, J.M. (2016). Multidomain Operations: A Subtle but Significant Transition in Military Thought. *Air and Space Power Journal*, Spring 2016, Volume 30, No. 1.

Sullivan, I.M., Bauer, J.C., Berry, E.L. & Shabro, L. (2017). Understanding Tomorrow Begins Today: The Operational Environment Through 2035. *Small Wars Journal (SWJ)*.

United Kingdom Ministry of Defence (UK MOD). (2014). *Future Operating Environment 2035*.

United Kingdom Ministry of Defence (UK MOD). (2020). *Multi-Domain Integration*. Joint Concept Note 1/20.

United States Army. (2020). *America's Army: Ready Now, Investing in the Future*. FY19-21 Accomplishments and Investment Plan.

United States Army Futures Command (AFC). (2021). *Future Operational Environment: Forging the Future in an Uncertain World 2035–2050*. AFC Pamphlet 525-2.

United States Army Training and Doctrine Command (TRADOC). (2018). *The U.S. Army in Multi-Domain Operations 2028*. TRADOC Pamphlet 525-3-1.

United States Army Training and Doctrine Command (TRADOC). (2019). *The Operational Environment and the Changing Character of Future Warfare*. TRADOC Pamphlet 525-92.

Watling, J. & Roper, D. (2019). *European Allies in US Multi-Domain Operations*. Royal United Services Institute (RUSI) for Defence and Security Studies, RUSI Occasional Paper.

Willis, C., Bayer, J., Kelly, J. & Anderson, S. (2023). A Hybrid Approach to Combat Simulation Experimentation, *Proceedings of the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC) 2023*, Paper No. 23106.