Vol. n. 6 • 2023 ISBN 979-12-985129-0-0

2023 Annual Review

NATO OTAN

MODELLING & SIMULATION
HONOS ALIT ARTES
CENTRE OF EXCELLENCE

NATO
Modelling & Simulation
Centre of Excellence

Published by NATO Modelling & Simulation Centre of Excellence, Rome, Italy.

Edition: VI (June 2024)

ISBN 979-12-985129-0-0

Printed in Italy.

Disclaimer

The CA2X2 Forum 2023 Paper Collection is a of the NATO M&S CoE product. It is delivered to give an outline of the CA2X2 Forum 2023 and resulting productions. It does not represent the opinions or policies of NATO and reflects independent analysis, opinion, and position of the authors.
Limit of Liability/Disclaimer of Warranty: NATO M&S COE Annual Review is a product of the NATO M&S CoE. It does not represent the opinions or policies of NATO or M&S COE. The views presented in articles are those of the authors.

Release

This document is approved for public release. Portions of the document may be quoted or reproduced without permission provided a standard source credit is included.

Published and distributed by

The NATO Modelling and Simulation Centre of Excellence
Piazza Renato Villoresi, 1
00143 Roma
Italy

Owner

Col. Francesco PACILLO, Director, NATO M&S COE, Rome, Italy

Coordinator

Lt.Col. Jiri NOVOTNY, Doctrine, Education & Training Branch Chief

Editorial Board

Lt.Col. Bradley KOERNER, Deputy Director

Lt.Col. Bernd WEISSENBERGER, M&S Services Branch Chief

Lt.Col. Jiri NOVOTNY, Doctrine, Education & Training Branch Chief

Lt.Col. Felice D'IPPOLITO, Concept Development & Experimentation Branch Chief

Lt.Col. Stefano CAMBI, Support Branch Chief

Lt.Col. Cristoforo RUSSO, Public Affair Officer

Contributors

Lt.Col. Piergiorgio VENTURA, Concept Development Section Chief (NATO M&S CoE)

Capt. Salvatore DE MATTIA, Concept Development & Experimentation Branch, Former M&S Enterprise Architect (NATO M&S CoE)

Lt.Col. Federico MAZZONE Simulation Services Section Chief (NATO M&S CoE)

Publisher

CWO Maurizio MIELE, Sim-based Education & E-learning Specialist

Table of Contents

Preface

Dear M&S Community of Interest,

I am pleased to introduce you to this collection of articles exploring the theme of "Modelling and Simulation as a Cross-Functional Enabler."

In today's interconnected world, where challenges and opportunities span across multiple disciplines, the role of Modelling and Simulation as a force multiplier cannot be overstated.

You will find a diverse range of perspectives and methodologies within the realm of Modelling and Simulation and we are delighted to present this publication, showcasing the latest advancements, innovative approaches, and practical applications in Modelling and Simulation.

Whether you are a researcher, a student exploring the intricacies of simulation, or a practitioner seeking practical insights, we trust that this collection will inspire and inform your journey in Modelling and Simulation.

We extend our gratitude to the contributors for their scholarly contributions and commend their dedication to advancing this field.

Happy reading!

Best regards

Col. Francesco PACILLO

NATO M&S CoE Director

Part 1:

NATO M&S CoE Annual Review

ELMO (Electromagnetic Layer for Multi-domain Operations) Developing and Testing Activities

LTC Piergiorgio Ventura, CPT Salvatore De Mattia

piergiorgio.ventura@mscoe.org,
mscoe.cde04@mscoe.org

NATO M&S CoE

Abstract

The electromagnetic environment is an essential element for the understanding and conduct of future military operations. Its transversal characteristic permeates the operational scenario in a multi-domain perspective and, therefore, the comprehension and management of this physical dimension is crucial.

The NATO Modelling & Simulation Centre of Excellence (M&S COE) is conducting a project called "ELMO" (Electromagnetic Layer for Multi-domain Operations), which aims to create a synthetic environment for the virtualization of the so-called ElectroMagnetic Spectrum Operations (EMSO). In this context, M&S expresses flexible characteristics for the implementation of complex electromagnetic multi-domain scenarios, able to make visible in the scenario what is not visible or detectable in a real world environment. This feature would simplify the understanding of the main electromagnetic spectrum parameters and enhance the operational and informative characteristics, which the electronic assets provide within the Electronic Warfare context.

The EM layer was built using the Software Tool Kit (STK), developed by the AGI Company, and MATLAB, developed by the Mathworks Company. The integration of the two tools was exploited to generate ad-hoc synthetic military components such as Jammers and Radar Warning receivers.

A specific scenario was then built in order to simulate a military EM environment, where the STK synthetic assets, such as satellites, radars and communication systems, interact with the military components developed in MATLAB. The EM layer generated by the MATLAB-STK integration successfully provides a comprehensive visualization over time of the entire electromagnetic spectrum on the battlefield.

The tests performed in a demo scenario with interacting objects virtually operating in a comprehensive EM environment proved the capability of ELMO to develop a complex framework suitable, not only for Commanders' decision making, but also for capability Development and Experimentation.

Keywords: Electromagnetic Layer, Multi-domain Operations, M&S, decision making.

1 Project Conceptual Idea

The conceptual idea of the ELMO project is described by an architecture that explains the functional interconnection of the main blocks used for the implementation. The modelling and simulation (M&S) architecture consists of the following elements of interest:

– Matlab/Simulink: used to perform the mathematical modelling of the fundamental electromagnetic blocks to build the virtual objects in the synthetic scenario. This modelling phase mainly focuses on the constitution of the functional and behavioral algorithms of the systems.
– AGI STK (Systems Tool Kit): used for the construction of the synthetic environment useful for scenario configuration and for electromagnetic simulations calculations. This is important for the definition of the electromagnetic component that, in military operations, affects the four fundamental domains.
– Matlab-STK interconnection: the project is based on dynamic and continuous data exchanging between EM (Electromagnetic) models synthesized in Matlab and simulation results provided by the STK tool. In particular, an interaction is carried out between the functional algorithms of the models and the real-time results of dynamic EM propagation provided by the simulators.
– Artificial intelligence: considering a possible long-term future development, it was

conceptualized to merge potentialities offered by artificial intelligence with the described project, creating specific neural networks in feedback with the synthetic environment. In particular, by receiving data from STK, the neural network could be trained using multiple simulations. Furthermore, the deductive results produced by the neural network, could provide, the configuration parameters of the EM models, maximizing an objective function that considers new threats, scenario parameters, level of effectiveness and level of interoperability to be obtained.

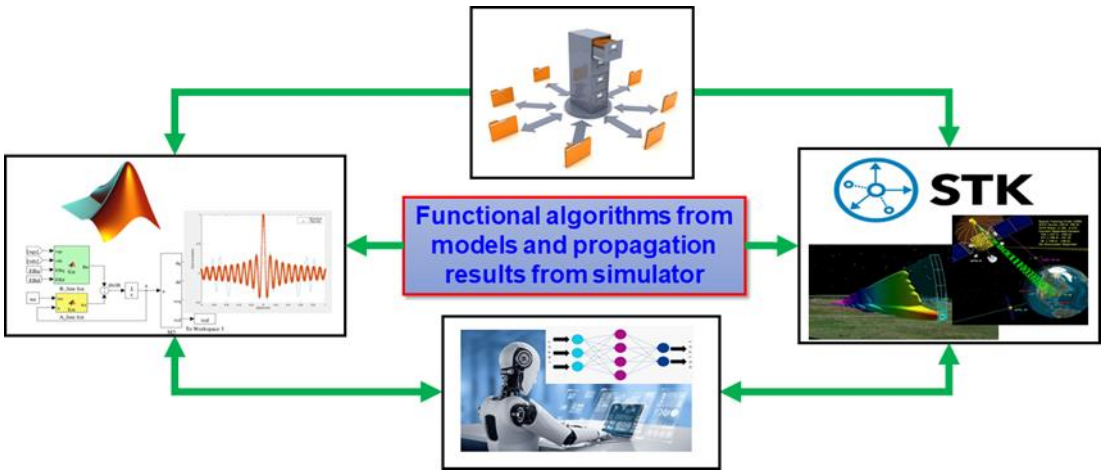


Figure 1: Conceptual idea of ELMO project (functional-logical architecture).

2 ELMO Data Integration

To make an example, in order to replicate a complete operating cycle of the proposed synthetic electromagnetic environment, the following logical operations are reported, based on the creation of two generic models of receiver and transmitter:

– The transmitter model is based on the programming of a specific operating algorithm, which, depending on the input parameters, will provide a specific output. In particular, the spectrogram matrix of the generated output signal (time, frequency, power) could be calculated as output.

– Through a connection between the STK tool and Matlab, made for example with special APIs (Application Programming Interfaces), with bi-directional characteristics (input/output), the matrix values of the output signal, associated with a specific virtual object inserted in the simulator, constitute the input of the antenna to proceed with the calculation of the propagation results. The bi-directionality of the mentioned connection between a mathematical simulator and a scenario simulator, with mainly propagative purposes, would allow generating results in terms of input data for further mathematical models.

– The receiver model is based on the programming of a specific operating algorithm, which, depending on the input parameters, will provide a specific output. In particular, certain behavioral feedback connected to the functioning of the modeled receiver device could be provided as output. This information will be transmitted within the synthetic environment to provide electromagnetic situational awareness and, possibly, carry out actions of an operational, technical and/or informative nature.

Therefore, Matlab/Simulink tool is a fundamental component of the ELMO project, especially in the modelling phase of peculiar EM systems, such as those used in a multi-domain electronic warfare context. In this case it is important to be able to create a behavioral model that reflects the functional logic of systems used in military operations (digital twin), defining the architectural blocks of a transceiver chain, except the radiating elements. In fact, the antennas will be inserted

directly into the virtual environment defined by STK, obtaining the radiation pattern desired for the specific electronic system to which it is connected.

The construction of models is a complex engineering operation because it is important to define a specific technical level on which to structure a logical operation of behavioral algorithm and to make a general-purpose model. This last feature is significant since it enhances the importance of the M&S tool applied to the military technological sector, ensuring, firstly, versatility of use through the virtualization process. Having a generic model available allows performing multiple technical-operational configurations, easily replicating different system architectures that could be assimilated to specific types of equipment supplied to the Armed Forces. Results obtained by the ELMO system are therefore related to a specific behavioral models of EM systems defined in Matlab and, therefore, take on greater technical-operational value with respect to EM layer in multi-domain military operations characterization. The versatility inherent in the models is also a key point in the experimental phase of ELMO synthetic environment, concerning the definition of systems of systems, such as gap filler type. The availability of electronic system models allows interfacing different apparatuses designed to cooperate for a common purpose, for example in Forces protection, and to exploit the ELMO synthetic environment to carry out technical and operational verifications, on the premise of any experimental activity in the field. This would have a benefit to analyze and maximize awareness of activities that, albeit with experimental premises, have a direct impact on operational and information structure.

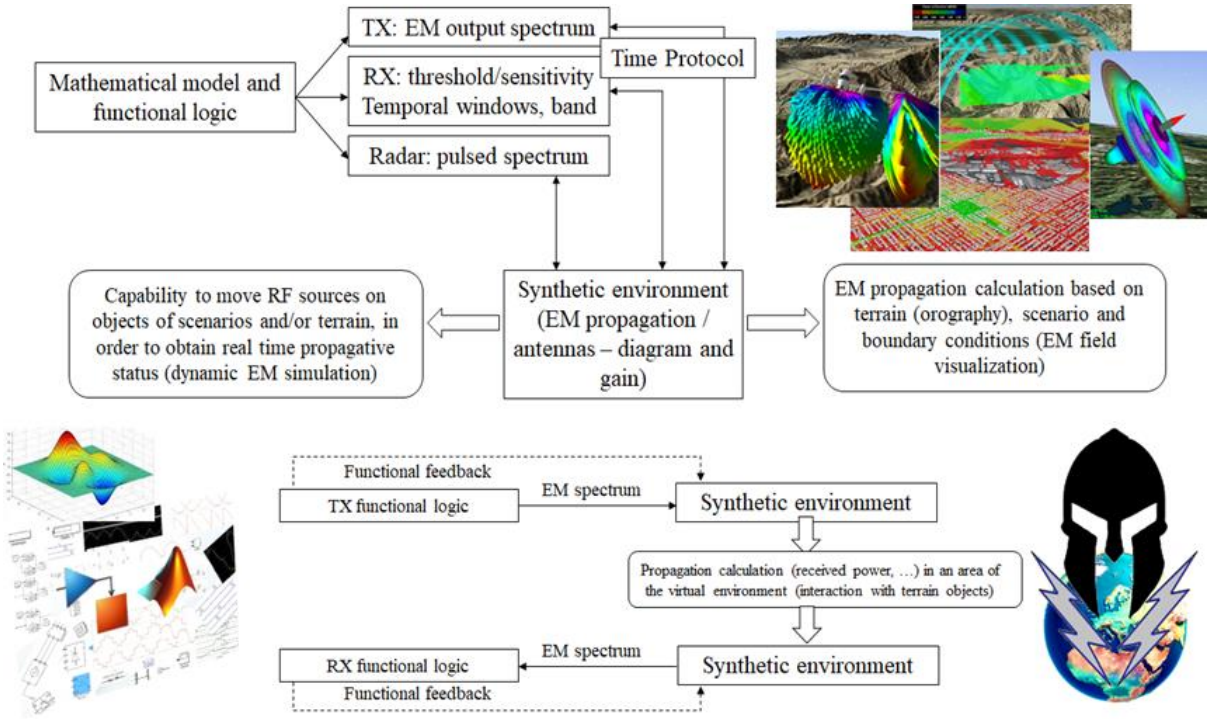


Figure 2: Flow chart for data integration implementation between the modelling and simulation component.

3 Project Applications

The creation of a synthetic environment for electromagnetic operations provides an increasingly crucial aspect for the fulfillment of multi-domain missions complying with progressive technological increase of threats, in a context of Electronic Warfare. The virtualization of the EM operating environment and interconnection intrinsic transversal feature with the main military domains allows performing a computer assisted

wargaming, in order to achieve the so-called best CoA (Courses of Action). In this regard, the conceptual analogy between a best CoA approach and obtaining technical, operational and information awareness aimed at defining the most effective electronic countermeasure (best countermeasure) is interesting. Once a scenario is virtualized, in terms of factions, types of platforms and systems, rules of engagement and objectives to be pursued, in line with the operation plan, by applying the concepts of computer-assisted wargaming, it is possible to develop technical and training skills to better manage the EM component, correlated to friendly and enemy Tactics, Techniques, and Procedures (TTPs). In addition, this situational approach would allow studying the perpetration of EM actions, from a multi-disciplinary point of view, mitigating any side effects (e.g. characterizing impacts in the cyber space used for the civil population).

The ELMO project can be used to integrate technical, operational and informative data. For instance, in an Electronic War context, the main identified impacts of using ELMO can concern using of electromagnetic countermeasures for Forces protection. The visualization and quantification of the electronic protection performance, albeit simulated, represents the starting point for expressing subsequent operational considerations and facilitate the decision-making process of the Commanders, providing information and feedback obtained from the electromagnetic component.

4 Conceptual ELMO Scenario

In order to implement a proof of concept for the project ELMO, a simulated scenario has been created. The main characteristics of this scenario are the following:

– The creation of a vignette in a multi-domain environment.
– The importance of the space domain for situational awareness increasing in the future operating environment.
– The key role of the electromagnetic spectrum operations for a military operation mission's accomplishment through the generation of tangible and multi-factorial effects on all the military domains, acting on operative and informative elements.

The space domain has been highlighted for its intrinsic peculiarities, which make it very suitable for new concept development and for mission conduction, involving non kinetic effects through the use, the management and the control of the electromagnetic spectrum.

The implemented scenario has been developed in Orlando city, in Florida, where a digital terrain has been created for the simulation analysis and propagation calculations. Generally, a synthetic terrain in a modeling and simulation tool is composed of:

– Shape files, which contain vectorial data for geometric elements definition, such as lines, points, polygons, etc.
– Elevation files, which can include ASCII values with information of the terrain profile.
– Raster files, which is a georeferenced picture of the selected terrain.

Each modelling and simulation tool manages the terrain generation files in different ways. In STK, a synthetic terrain for analysis has been created from a jpeg file. In addition to the terrain file, a satellite photo has been overlapped to have a fully visualization of the synthetic scenario which is going to be created. In STK, it is also possible to add buildings present in a city, configuring a shape file containing, for instance, the polygons describing the buildings. The described operations have been done in Orlando city, in order to set the virtual terrain for analysis and for visualization of the simulation in a 3D perspective. Moreover, has been inserted a 3D tile object in the simulator, which simulates a military headquarter, in Exton, USA.

After the synthetic terrain definition, the virtual

mission has been configured and, consequently the digital platforms with several attached devices. To better understand the implemented scenario, it is important to specify that the units are presented in two factions, blue and red forces, according to the electromagnetic military actions that are going to conduct in the synthetic environment.

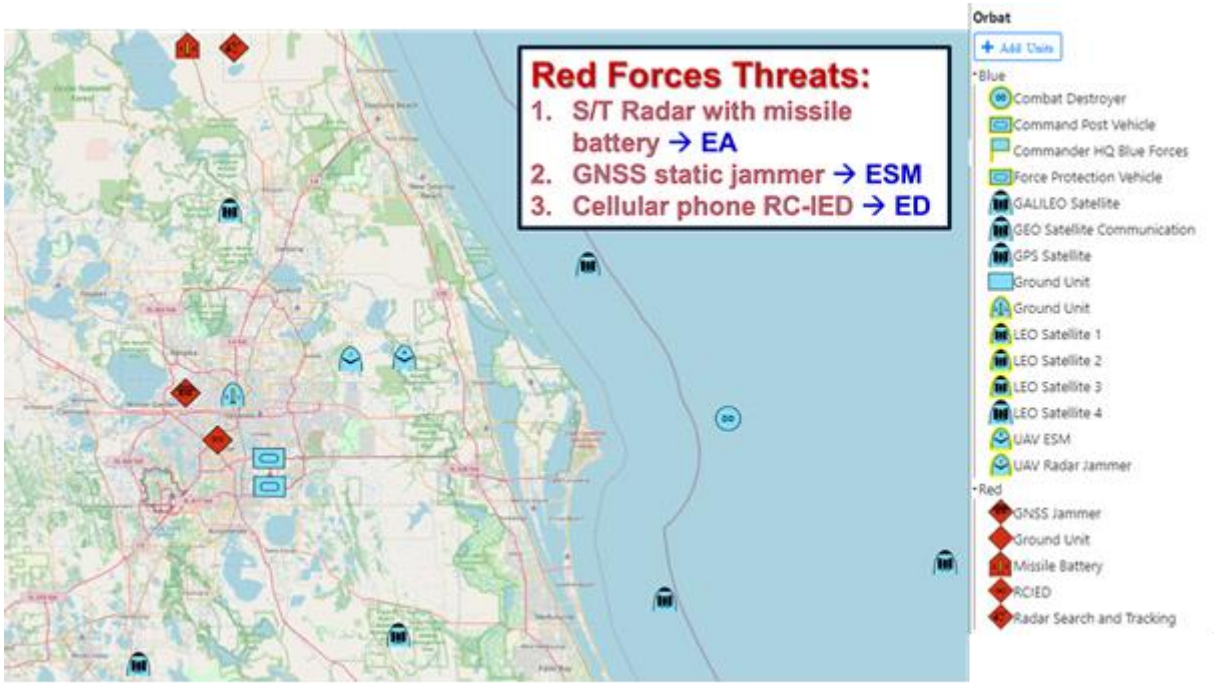


Figure 3: Scenario representation including blue and red forces units.

This scenario contains several EMSO actions, in particular:

– EA (Electronic Attack): the UAV performs an EA activating the on-board jammer toward the enemy radar;
– ESM (Electronic Support Measurement): the ground master station is able to send suspicious threats detected after a spectrum monitoring to LEO constellation for direction finder to geo-localize the enemy radar. In addition, the UAV is able to monitor the electromagnetic spectrum in an urban area, in order to send information to a ground vehicle jammer;
– ED (Electronic Defense): the ground vehicle is equipped with a hybrid jammer, automatically configuring system's reactive phases through UAV ESM actions and with a pre-programmed waveform in the active phases. These actions can be performed both in time sequence and in time parallel.
– Electromagnetic interoperability:

o Time domain: 1PPS generated by GPS receivers of the platforms allows creating a synchronized time protocol regardless the military domain where the platform operates;
o Modulation: the use of Galileo signal for Positioning purpose allows having a lower interference with respect to a high power and continuous wave L1 GPS jammer;
o Antenna beam forming: the ability of a simulated phased array to create a null finder toward an interference source, providing, at the same time, maximum gain in satellite direction, which can improve the Signal to Noise Ratio of the communications.

5 External Matlab Models

Matlab tool has been used to build digital models of electromagnetic systems, which are not available in

STK. In particular, STK despite provide many embedded models for different electromagnetic systems, is not able to cover the overall spectrum of military electronic devices that can be employed in the future operating multi-domain environment. In particular, the military electronic devices are often designed as system of systems, implementing custom algorithms and based on specific logic connections and hardware architecture. For instance, at the same transmitter power and bandwidth, two different electronic counter systems designed with two different circuital architectures and with two functional logics, can show a wide difference performance in terms of level of effectiveness against the same threat, in the same scenario boundary conditions. Another important aspect to consider is the electronic waveform programmed and implemented inside the system defining methods for receiving and transmitting electromagnetic signals.

In this context, Matlab is considered as an expert modelling and simulation system where, through a code-based approach, it is possible to create a digital model of any specific device, which can be used in the EMSO context. The models are created as digital twin of a real system, in terms of behavioral and functional algorithms, for experimenting and verifying many results, obtained implementing different technical or operative configurations in the synthetic environment.

Among the models created within the ELMO project, two digital models of systems are reported below, in order to better clarify the concept expressed for the M&S supporting EMSO and to show potential capabilities defined by Matlab and STK integration. These Matlab models have been based on a specific and simple characteristic, which links the current and the future digital systems in the virtual environment: the flexibility of a general-purpose architecture, which represents the cornerstone for further considerations and experimentations. The achievement of the general-purpose characteristic is essential in a modelling and simulation project, since, in this way, it is possible to test many hardware and software configurations of the same systems, by changing input variables or applying minor changes in Matlab scripts, allowing the conducting of a multi-factorial analysis through the simulation. Furthermore, the need to be versatile and general purpose is crucial in the concept development and experimentation field, mostly for studying and analyzing a complex problem using a comprehensive approach method.

As first proof of concept, a military jammer has been created in Matlab, which integrates different functionalities:

- Active jammer: a device that involves only transmitter chains and it works, usually, with an electronic waveform created in pre-mission phase, according to radio frequency information of operation area.
- Reactive jammer: a device that involves both transmitter and receiver chains, able to create a radio frequency spectrum in response to the electromagnetic environment in the operation area, according to configured timing and frequency parameters.
- Hybrid jammer: a device that can perform both active and reactive phases, using a single chain (time sequence) and/or a multi chain configuration (time simultaneity).

The realized digital model of jammer system defined in Matlab corresponds to a hybrid system, since this is the most complex architecture, in terms of functional phase's integration. For this reason, a specific setting of the input and control variables allow to simulate also an only active and an only reactive jammer. Furthermore, in this digital model is possible to choose the hardware configuration of the electronic counter measure system, in terms of number of transceivers and power amplifiers, and the software configuration expressed as configuration typology (single or multiple chain). These technical aspects make the model general-purpose and its scripts composition gives usage modularity, providing an easy way to create different system architectures.

6 Scenario Different Course of Actions

The modelling and simulation supporting electromagnetic spectrum operations is a key technology, which allows studying and analyzing how this operating environment will influence transversally the military domains, in terms of informative, technical and operative aspect. In this scenario, although the multi-domain assets represented, the space domain has been highlighted, through which, in conjunction with the electromagnetic environment, it is possible not only to increase the situational awareness, but a comprehensive operative management of the future battlefield.

The synthetic scenario allows reaching a high level of versatility, meaning that by changing particular configuration variables of systems' models it is possible to obtain completely different operative results. Different results will lead to several courses of action, which correspond too many scenario ramifications. The following situations can be easily generated and verified.

Master station does not receive suspicious frequencies: the LEO satellites constellation cannot be configured with received frequency and the estimation algorithm cannot be processed. Any UAV missions in the operating area can be detected and be destroyed by radar guided missiles.

Master station receives suspicious frequencies: the LEO satellites constellation can be configured with received frequency and the estimation algorithm can be processed. As a result, an estimation point is obtained associated to an uncertainty area.

UAV jammer is not able to inhibit enemy radar: the on-board single frequency jammer is connected to a dynamically change antenna, pointing to the estimated point of the target and whose directivity is proportional to maximum obtained uncertainty error. The uncertainty level of the ELINT system is able to change automatically jammer antenna gain and directivity, so it means that the EIRP can be strongly affected by FDOA results' precision. The inhibition of the radar is connected to the jammer parameters, to radar technological architecture implemented in the model and to the radar cross section of the target asset.

UAV jammer is able to inhibit enemy radar: the two UAVs of blue forcers are not detected, hence not destroyed, by enemy radar thanks to the electromagnetic attack performed through the UAV jammer. The search function is completely jam and the subsequent tracking phase for missile launching is not activated.

Galileo L1 modulation is affected by jammer: the use of a multi-constellation receiver on-board UAV ESM is a very important aspect in this simulation. A specific BOC modulation configuration has been chosen for satellite transmitters, in order to highlight Galileo signals resilience in a noisy environment (narrow band L1 jammer signal) with respect to GPS ones. The capability to use Galileo allows to UAV ESM to send the precise target (enemy GPS jammer) position to conduct a kinetic action on it and restore GPS receivers in the operating area.

UAV ESM detects BTSs and MSs: one of the mission performed by UAV ESM is to monitor radio frequency spectrum, in specific bands, over a high-density urban area. This electromagnetic surveillance is part of the a multi-domain architecture to implement a hybrid jammer waveform, where receiver stage has been conceptually de-localized with respect to the ground vehicle used for electronic force protection. The ESM receiver electronic configuration (e.g. instantaneous bandwidth and scanning technique) and the collected signals samples are fundamental for subsequent electronic defense actions. Based on an incorrect intelligence information or an incorrect model configuration, the effective threat signal cannot be detected or too many (environment) signals are collected. The latter situation is typical in an electronic support measure action performed in an urban

environment and can result a jammer device to be completely ineffective, since it needs to spread its (limited) resources over many suspicious threats.

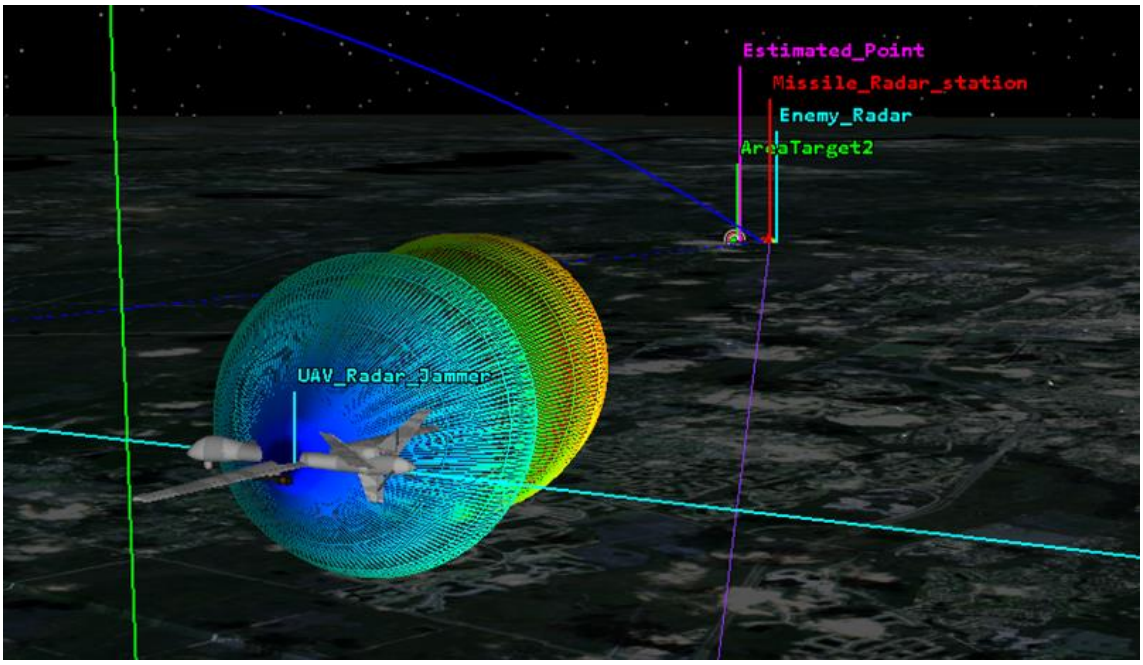


Figure 4: UAV radar jammer 3D object and antenna pattern view.

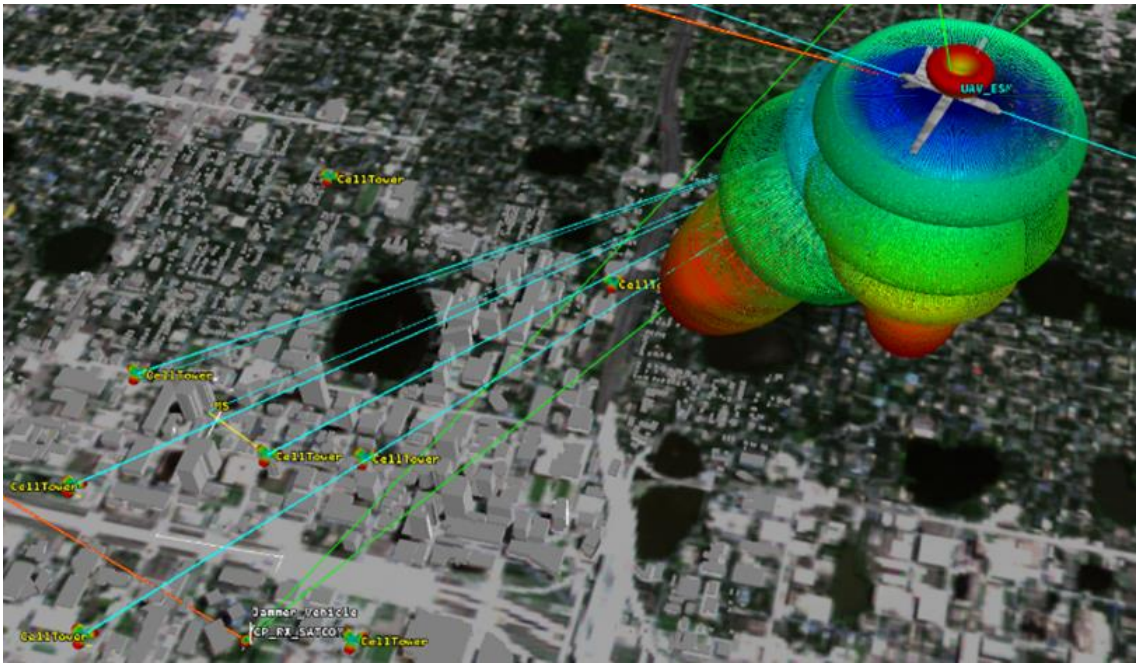


Figure 5: UAV ESM 3D object and antennas pattern view.

GPS jammer is not destroyed: the enemy GPS L1 jammer is placed in the operating area in order to avoid use of PNT devices by blue forces. The GPS jammer continuously disturb the electromagnetic environment making ineffective blue forces devices using L1 signal functionalities. In this situation, the ground vehicles mission is performed anyway, albeit with technical and operative limitations. As result, the jammer reactive part is filled with blank information,

generating an only active waveform. The active waveform is configured in pre-mission phases and it is fixed, meaning that there is not a dynamic spectrum adaption according to the specific electromagnetic environment of the operating area. Since the resources of the jammer are limited in time, in frequency and in power, using an active waveform needs to have suitable informative support, in order to be effective inhibiting several possible threats. Mostly in an urban scenario and for multi-purposes devices (e.g. cellular phones), it is very difficult to have a priori detailed information concerning radio frequency possible threats.

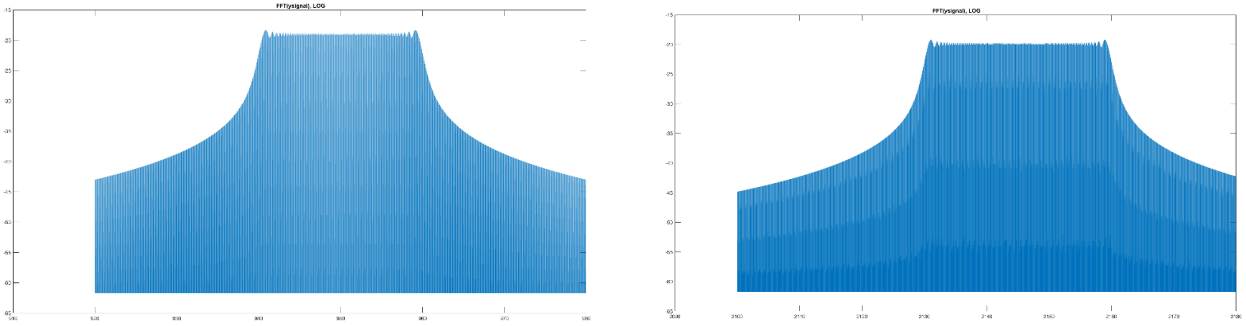


Figure 6: Matlab jammer external model spectrum in active waveform mode (2G left and 3G right).

GPS jammer is destroyed: the multi-domain electronic warfare system works properly, meaning that UAV ESM and ground vehicle are perfectly synchronized in time, sharing the same time protocol for data exchanging. The ground vehicle can receive data collected after UAV ESM action over the city, automatically generating its waveform in hybrid mode (reactive and active at same time). Jammer reactions are created on the detected frequency contributions, dynamically adapting the system's resources and transmitting an electromagnetic signal with specific characteristics, according to model configuration.

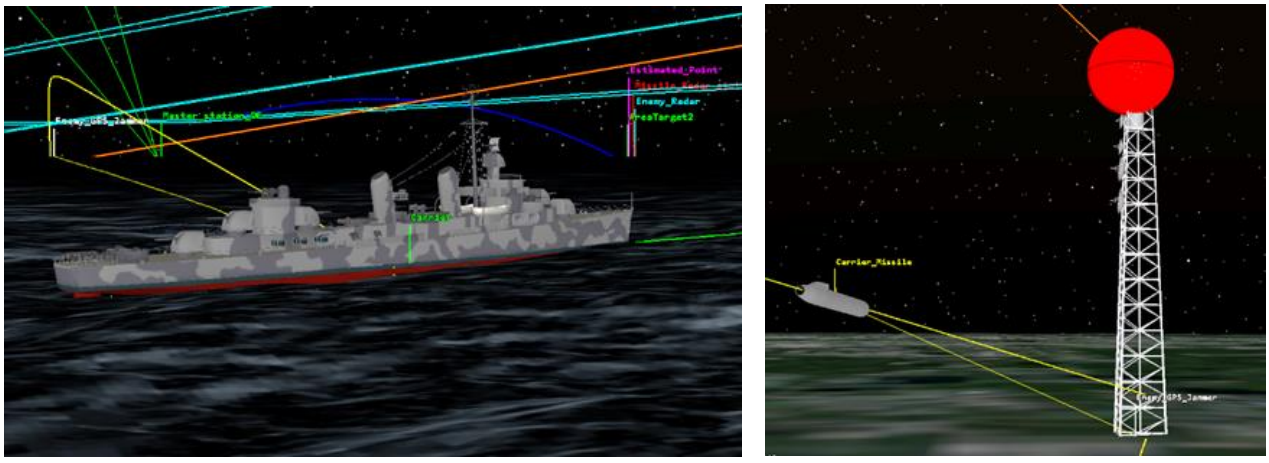


Figure 7: Military ship (left) and tomahawk missile (right) launched towards GPS jammer station 3D objects' view.

Ground vehicle hammer inhibits 2G/3G threats: depending on jammer waveform transmission (hybrid or purely active) the effects on radio controlled improvised explosive device threats can be very different. In this context, the obtained results are ranges of effectiveness with respect to the target vehicle (command post with satellite receiver), calculated in this specific scenario and using both J/S and Eb/ (N0+Io) thresholds. These thresholds have to be set correlating to threat's signal characteristics to jam (e.g. modulation, frequency, multiplexing, data rate, etc.). For these reasons, according to the jamming thresholds set in this scenario, it is

possible to verify performance differences of using an active or a hybrid jammer waveform. At the same power, frequency, timing system resources, to have a theoretical waveform configuration better than another is impossible, since the informative, operative and technical variables that concur to force protection level are too many and not known a priori. Therefore, a creation of a synthetic environment able to model and simulate these peculiar aspects is important to manage the current and the future electromagnetic spectrum operations, increasing operational value of the M&S supporting military sector, through a representation of these non-kinetic effects.

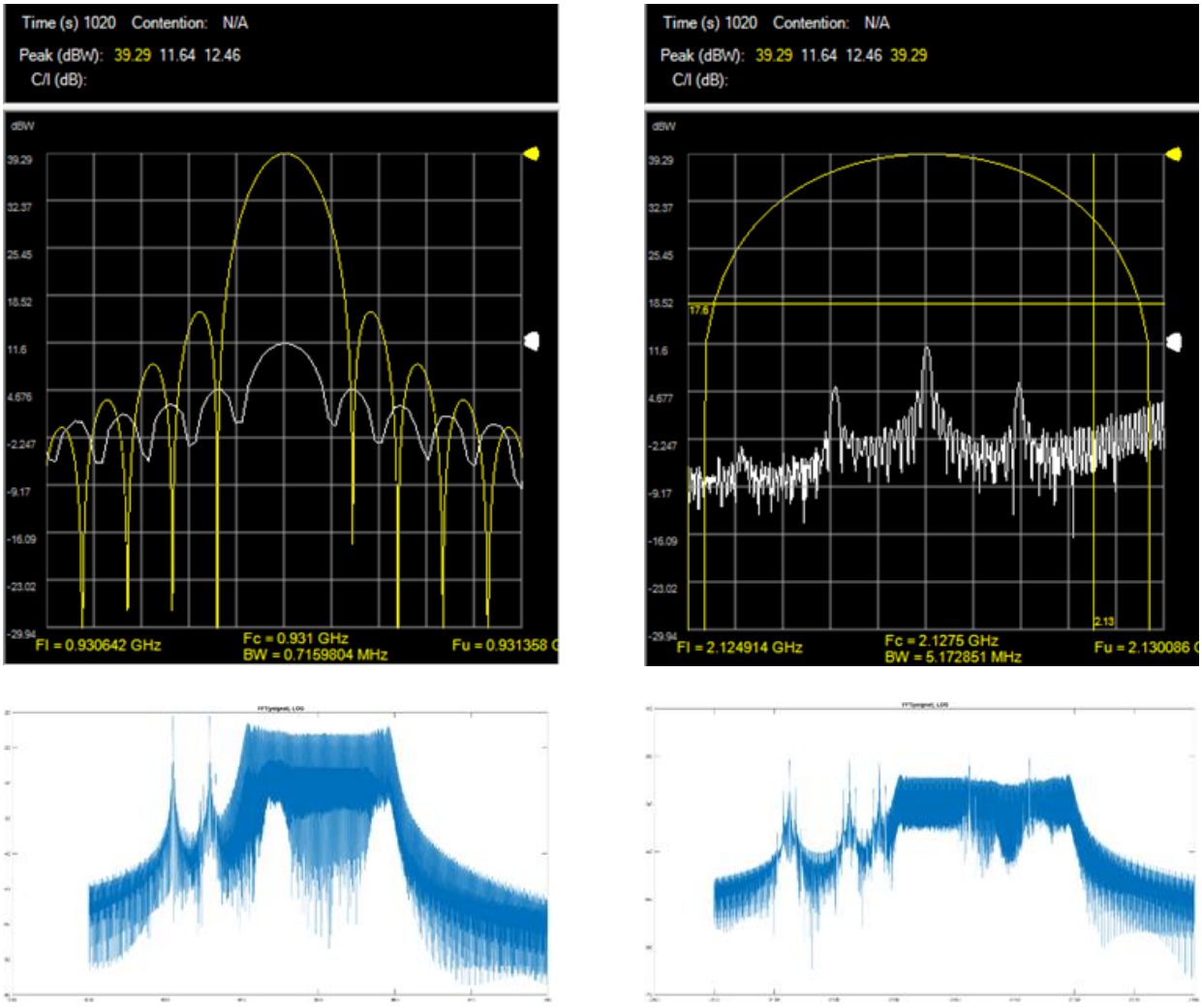


Figure 8: STK spectrum analyser and Matlab jammer external model spectrum (see text for details).

In figure 8, you can visualize these different performances. In details, STK spectrum analyser in MS GSM receiver is visible on the top-left, and MS UMTS receiver is visible in the top-right, showing the jammer waveforms (white) and cellular communication channels (yellow). Matlab jammer external model spectrum in hybrid waveform mode is shown for 2G on the bottom-left and for 3G on the bottom-right.

Ground vehicle's satellite receiver communicates with HQ: depending on jammer waveform transmission (hybrid or purely active) the effects on the command post ground vehicle's satellite receiver can result very different. A more effective jammer system and its waveform can unintentionally increase the noise interference level towards a friendly communication device. In this case, since the inter-vehicular distance is very close, in order to provide better electromagnetic protection by jammer actions, and due to a very low level

received signal coming from satellite downlink connection, it is very important to simulate the devices electromagnetic interoperability. The interoperability evaluation is obtained by calculating quality of satellite communication, according to the vehicles' mission, interference contribution and satellite communication receiver configuration. This configuration is conducted essentially by changing phased array antenna pattern, defining a null finder capability, showing its effect on radio frequency source attenuation with respect to desired signal.

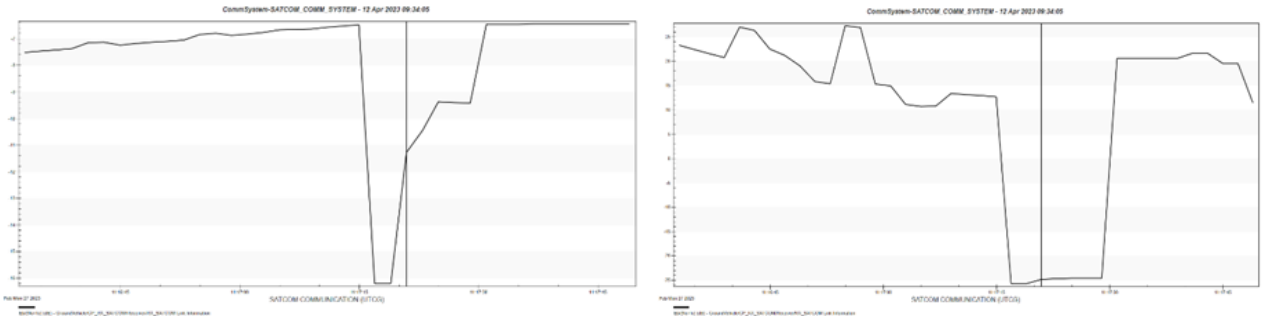


Figure 9: STK graph of satellite communication Eb/(N0+I0) parameter configuring the phased array antenna without null finder capability (left) and with null finder capability (right).

The electromagnetic interoperability has been studied using the Eb/(N0+I0) temporal envelop, shown in two dirrent situational scenarios:

1. Phase array receiver antenna does not implement the null finder functionality: maximum Eb/(N0+I0) value is around -8 dB, meaning that there is no satellite communication, since the downlink path is distorted by jammer interferences;

2. Phase array receiver antenna implements the null finder functionality: maximum Eb/(N0+I0) value is around 27 dB, meaning that there is satellite communication and the command post ground vehicle is able to receive all the military information by military HQ. In this case, the jammer interferences in L band are strongly attenuated by antenna radiation diagram.

Therefore, by using the null finder algorithm capability on a phased array antenna, it is possible to earn around 35 dB on Eb/(N0+I0), meaning that the satellite communication using the GEO satellite transponder is affected by a low bit error rate.

In STK simulator, a phased antenna model has been implemented using a MVDR (Minimum Variance Distortionless Response) beam former algorithm. Beam former algorithm can compute the weights of each array element, for shaping antenna's gain pattern. MVDR changes the amplitude and phase across the array elements to steer and shape the beam as well as the nulls. Therefore, the MVDR goal is to minimize the variance of the beam former output. If the noise and the underlying desired signals are uncorrelated, as is typically the case, then the variance of the captured signals is the sum of the variances of the desired signal and the noise. Hence, the MVDR solution seeks to minimize this sum, thereby mitigating the effect of the noise. In this model, a MVDR constraint of 3 dB has been set. This value is used to constraint the amount of main gain reduction, which can take place to null interference.

The decisional branches of this scenario are managed by Matlab code, whose effects are projected into STK simulator, structuring a conceptual decision tree diagram based on communication parameters thresholds. To evaluate a quality of a link budget, Eb/N0 (in normal situation) and Eb/(N0+I0) (in presence of radio frequency interference) have been calculated and verified. On these parameters, the thresholds have been set considering a common BER value (e.g. 1e-6) and considering the modulation chosen for communication links. This approach has been adopted to simply the decision tree conditional phases, although it can be easily modified with different threshold values and BER considerations.

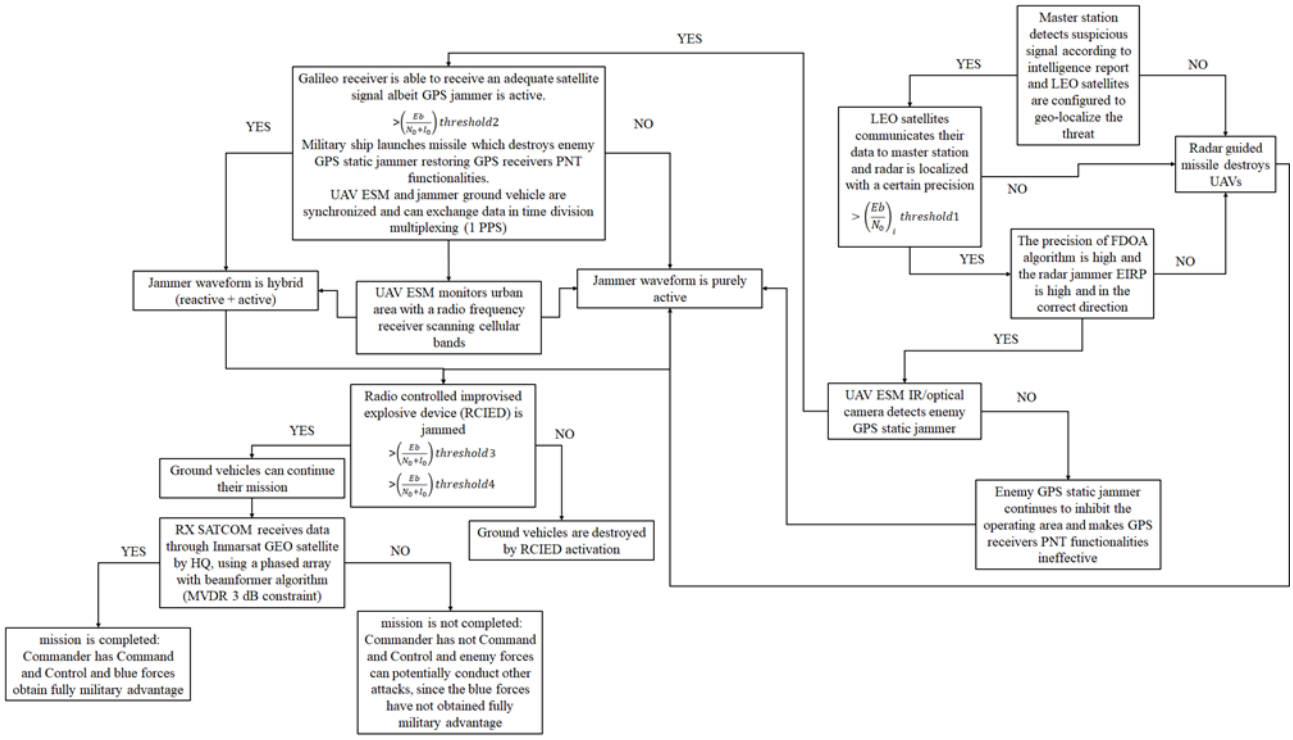


Figure 10: Scenario's decision tree developed based on conditional thresholds.

4 Conclusions

The Modeling & Simulation in support of electromagnetic operations could also allow system configurations, in order to understand how to counter new electronic threats, studying and characterizing, for example, the effectiveness of gap filler systems. The creation of a complex urbanized virtual scenario is an essential component in the analysis of the technical-operational effectiveness of the electromagnetic devices used in operation, both from a spectral and a physical point of view. In particular, the physical virtualization of the surrounding environment allows simulating the main propagative effects provided by the physical objects defined in the scenario, whose understanding and analysis allows obtaining a quantification of the performance effectiveness, in relation to the maximization of the efficiency of the technical and operational processes of the employed electromagnetic equipment.

Concerning to the ever-expanding technological dynamism within the military context, a winning approach will surely be a comprehensive one, where military professionals able to carry out interdisciplinary and heterogeneous analysis and assessments will increasingly a have fundamental role, in order to synthesize, within a single technical direction, declinations and operational applications. Shortly, it will become essential to model and to manage the future complex military challenges within a vast and diversified technological substrate, through capability developments characterized by a high technological level but with a direct and simple operational projection to support military operations.

About the Authors

LTC (ITA – OF4) Piergiorgio Ventura

He is graded in physics in 1998 with a specialization in Nuclear Physics. He then joined the Italian Army in 1999 with the rank of Lieutenant and start working within experimental firing ranges where missiles, weapon systems and ammunition were tested. After taking a PhD in quantum electronics and plasma physics in 2010, during which a remote sensing detection system to detect and identify

chemical compounds, based on optical detection, was developed, he started working in the CBRN field for research, testing and procurement activities. Since January 2022, he is employed at M&S COE as M&S Concept Development Section Chief, where he is trying to develop new concept considering his expertise.

CPT (ITA – OF2) Salvatore De Mattia

He is an electronic engineer of the Italian Army, with specialization in radio frequency circuits. He worked at NATO M&S COE from October 2020 to October 2023, in the Concept and Experimentation Branch. In his first position, he was in charge of the Electronic Warfare (EW) sector, where he is mainly involved in the jammer systems configuration, for the protection against the RCIED (Radio-Controlled Improvised Explosive Device) threat. During this period, he worked both in Italy and abroad in various Operational Theaters in Afghanistan, Somalia, Lebanon (UNIFIL) and Iraq. He worked, as Subject Matter Expert, on projects concerning the use of Modelling & Simulation for Robotics and Autonomous Systems (RAS) and EMSO (Electromagnetic Spectrum Operations).

References

[1] Lt Col Tim Vasen (GE AF), *Resiliency in Space as a Combined Challenge for NATO*, Joint Air Power Competence Centre, from https://www.japcc.org/wp-content/uploads/Resiliency-in-Space-as-a-Combined-Challenge-for-NATO.pdf

[2] Harry L. Van Trees, *Optimum Array Processing Part IV of Detection, Estimation, and Modulation Theory*, Pg. 439

[3] K. C. Ho, Y. T. Chan, *Geolocation of a known altitude object from TDOA and FDOA measurements*, IEEE Transactions on Aerospace and Electronic Systems, 33(3):770–783, July 1997.

[4] Bakker PF, *Effects of radio frequency interference on GNSS receiver output*., Delft University of Technology. TY - BOOK, DOI:10.13140/2.1.1355.7763 (2006)

[5] Misra R, Palod S, *Code and carrier tracking loops for GPS C/A code*, International Journal of Pure and Applied Sciences and Technology 6(1):1-20 (2011)

[6] Russon MA, *Wondering how to hack a military drone?* It´s all on Google; [accessed 2016 Nov 04]. From http://www.ibtimes.co.uk/wonderinghow-hack-military-drone-its-all-google-1500326 (2015)

[7] Scott L, *Approaches for Resilient Positioning, Navigation and Timing (PNT)*, Association of Old Crows; [accessed 2015 Oct 15], from http://crows.org/item/gps-interference-origins-effects-and-mitigations.html (2015)

[8] The Royal Academy of Engineering, *Global navigation space systems: reliance and vulnerabilities*. London (England) - (2011)

[9] European Space Agency, *About the European GNSS Evolution Programme,* from http://www.esa.int/Our_Activities/Navigation/GNSS_Evolution/About_the_European_GNSS_Evolution_Programme, accessed on 20.12.2017

[10] Microsemi Corporation, *Timing and Synchronization for LTE-TDD and LTE-Advanced Mobile Networks*, whitepaper, 2014

[11] Fasoulas Aristides Ioannis, Boger Dan C., Gates William R., *Inmarsat communications system: a systems approach*, Monterey, California. Naval Postgraduate School from https://archive.org/details/inmarsatcommunic00fasopdf

[12] L. Yang, M. R. McKay, R. Couillet, *High-Dimensional MVDR Beamforming: Optimized Solutions Based on Spiked Random Matrix Models*, IEEE Transactions on Signal Processing, vol. 66, no. 7, pp. 1933-1947, 1 April, 2018, doi: 10.1109/TSP.2018.2799183.

[13] https://help.agi.com/stk/

[14] https://en.wikipedia.org/wiki/Verification_and_validation_of_computer_simulation_models

Modelling & Simulation in Support of a Comprehensive CBRN Layer Development

LTC Piergiorgio Ventura, CPT Salvatore De Mattia

piergiorgio.ventura@mscoe.org,
mscoe.cde04@mscoe.org

NATO M&S CoE

Abstract

Modelling & Simulation in support of CBRN and Environmental Protection has not been fully exploited to its maximum potential in the military domain; namely, Education and Training (Exercises), Support to Operations, Planning (Course of Action Analysis), Execution (Decision Support), Mission Rehearsal, Concept Development & Experimentation (CD&E) and Procurement. Many CBRN tools already exist, such as those providing models to simulate the dispersion of CBRN Agents, or the wearing of IPE during training. However, a comprehensive list of these types of tools, fully integrated to maximize its effectiveness, is still missing.

This innovative approach, which integrates existing tools and provides those not yet developed, represents a powerful M&S asset to fill the gap of this military problem. The purpose of this project was to develop and test, in a synthetic environment, a CBRN layer integrating the available tools, such as CBRN Analysis or Computer Generated Force Tools, to maximize their capabilities and to perform missing CBRN related activities. For example, to determine the effects of chemical compounds on military units or developing a plug-in software to integrate the existing database and perform specific computations.

The CBRN layer will be developed using the SWORD simulation software developed by MASA Company and the CBRN Analysis developed by BRUHN NEWTECH Company. The scenario will be built to simulate a synthetic CBRN environment with contamination and diffusion data. CBRN Analysis will provide this data and the military assets will be created by SWORD with the final objective of giving the Commander a comprehensive visualization of the CBRN framework in the battlefield.

Keywords: CBRN layer, M&S, Integration, Comprehensive Approach.

1 Introduction

CBRN Military readiness is critical to both the NATO and the Partnership for Peace (PfP) countries. For this reason, several working groups (WG) within the NATO community have developed numerous documents (STANAG, STANREC, Standard Related Document, etc..) which try to fulfill needs concerning Detection, Identification and Monitoring of CBRN threats, Protection, Hazard Management, Training and Education, CBRN Doctrine and Terminology. In addition, environmental protection is increasingly becoming an important activity to be taken into account during NATO led activities, especially during "non art. 5" operations. Also for this field, some WGs have developed the relative doctrine. In other words, CBRN and environment related military activities have been exploited quite deeply covering the full DOTMLPFI approach.

Nevertheless, CBRN and Environmental M&S have not been fully exploited within its potential in the military domain, namely, Education and Training (Exercise), Support to Operations, Planning (Course of Action Analysis), Execution (Decision Support), Mission Rehearsal, Concept Development & Experimentation (CD&E) and Procurement. Many tools do exist, such as models to simulate the dispersion of CBRN Agents, or the wearing of Individual Protective Equipment (IPE) during training and many others. However, there is not a full integration of these tools, and many are still missing. A comprehensive approach, which integrates all existing tools, including any that are missing, could be a powerful way to cover this important gap. A description of what can be included in this future CBRN layer, starting from

the existing M&S tools (GAP analysis) is provided in this paper, including a road map to achieve it.

2 What Could Be Provided by a CBRN Layer (Nice to Have)

A brief description of the new integrated approach is described as follows.

A CBRN and Environmental specific layer is added to the virtual reality, so that in the case of a CBRN release or environmental problem, whatever the type and origin, can be properly modelled and thus simulated, considering the effect of the others layer (e.g., detailed weather conditions). The effect of this layer is then used for:

– Education and Training (Exercise): the ability to give orders properly (and timely) to don or undon Individual Protective Equipment (IPE) and/or activate Collective Protection Equipment can be exploited. If you do not give the order to don, you lose personnel and capabilities, but on the other hand, if you are too cautious your ability to operate is reduced (simulation should include degradation as provided by STANAG at ref. [2]) resulting in lost personnel and capabilities for other reasons on the battlefield. CBRN personnel can be trained so that they have to decide how to operate to evaluate and mitigate risks (where to send sampling teams, where to organize decontamination activities, etc.). Many advanced tools can be built (e.g. considering the efficiency of the filtering systems depending on the concentration of chemical compounds over time, the filtering saturation expected, and the route employed by the vehicles or personnel, etc.).
– Support to Operations: The CBRN and environmental layer can be used the same way to make real decisions, so that in case of a real CBRN release the dispersion model and consequent simulation can be used to decide which troops should don IPE or not. This would take into account their degradation in terms of operability, need to change routes depending on the concentration of the CBRN threat, to verify the performance of the protection system (e.g. filter residual protection after exposure to a concentration as a function of time) and many other operative decisions. The environmental side of the simulation can be used to calculate the environmental problems arising during operations to take the proper decision to mitigate the effects.
– Planning (Course of Action Analysis): In the same way, several different scenarios can be employed to properly address the decision making process for CBRN experts and decision makers in general.
– Mission Rehearsal: wherever and whenever a risk of a real use of a CBRN agent or the risk of a CBRN release is involved (e.g., an action where a chemical plant or depot is hit or destroyed), proper mission rehearsals should include actions to take to mitigate the CBRN risk.
– Concept Development & Experimentation (CD&E): new capabilities in the CBRN field should be analysed with all CD&E M&S tools (Visualization, Conceptual Modelling, Simulation-based Experimentation, Analysis) in order to test disrupting technologies in this field (e.g. remote sensing, use of UAV integrated detection systems, widespread mini-detectors, etc..) or new doctrine (e.g. Multi Element Recce Team).
– Procurement: the capability of a new CBRN system (Protection, Decontamination, Detection, etc.) can be exploited with this approach, simulating its real use in a contaminated environment.

In particular, the requirements are as follow:

– develop the capability to calculate, properly and realistically, the behaviour of a CBRN agent in the environment in order to replicate it in a synthetic environment;
– federate the tool used to generate the CBRN agent dispersion, generally called an expert system, with a Computer Generated Forces (CGF) System able to replicate military behaviour. This integration will allow the visualisation of the CBRN Agent specific effects on the battlefield in real time.
– Make the simulation as much realistic as possible by using the above mentioned CBRN effects obtained with our M&S tools and combine them with the aspects already determined for civilian applications perfectly described in the document "Modeling and Simulation of Hazardous

Material Releases for Homeland Security Applications " (ref. [1]).

Other aspects, closely related to military applications to consider are:

– physical effect on personnel protected with IPE, inside a shelter or a vehicle, with CBRN filtration system or not, etc. In more advanced version, the system should take into account the effects on human beings, e.g. LD50 (Lethal Dose for 50% people) provided by STANAG in ref. [3]. The number of death, wounded and inability to fight of personnel should be as precise as possible. A properly developed tool to be connected with HLA, modifying also CBRN NET FOM, could be a solution.
– physical effects on personnel wearing IPE already considered in other M&S tools, but not verifying the realism of the activity, also considering the STANAG in ref. [2]
– CBRN platform protection, filter duration/filter saturation related to time, route and speed.

From the decision maker point of view, the system should help the commanders to take decisions or verify the decision taken during training. Among the decisions that can be taken, the following are relevant:

– Determine where and when military personnel or civil servant should don IPE;
– Determine where and when military personnel or civil servant should not don IPE anymore;
– Determine mask's filter duration as a function of the concentration and time of exposure (integral C(t)dt > Filter saturation);
– Determine where and when Vehicle should employ CBRN Filtration Systems;
– Determine where and when Vehicle should stop employing CBRN Filtration Systems;
– Determine vehicle's filter duration as a function of the concentration and time of exposure (integral C(t)dt > Filter saturation);
– Determine the best route (as a function of speed, also) to go from a starting point to an ending point avoiding as much CBRN contamination as possible;
– Determine the burden and operativity limitation for personnel, vehicle or other equipment during CBRN exposure (it exist to some extend); consequently, determine the effect on operation (training, exercise, mission rehearsal) so as to assess the risk balance;
– Determine deaths and casualties if CBRN procedures are not well followed during virtual exercise (e.g. IPE don or not don, filters durations, filtration systems employed, etc.).

In order to take into account also the needs of the specialist CBRN troops and technical personnel, also the following capabilities should be taken into account:

– Determine where to send SIBCRA Teams, UAV, UGV or any other useful tools to detect the threat, sample soil, water or gas, so as to confirm the predicted contaminated area and delimitate the exact contour;
– Use the information provided by detectors and sampling analysis to adjust M&S input so as increase the reliability of prediction on contaminated areas.
– Determine weather effects on CBRN Agents, such as degradation of chemical compounds due to the temperature, direct sunlight, water, etc... or the survivability of spores, viruses and bacteria.

3 Analysis of Experimental Activities

There are too many M&S tools to analyse all of them from a CBRN perspective. Each tool would need to be explored to fully understand it's potential. For this reason, attention was focused only to the experimental activities already performed, which demonstrates the real capabilities of "Expert Systems", used for CBRN activities, and CGF tools and thus their ability to exchange effectively information which could be used to generate effects.

Among experimental activities, several M&S group were organized along the years by NATO STO in order to deal with CBRN activities. Originally, NATO MSG-049 - Modelling and Simulation System for Emergency Response Planning and Training in 2011 identify a lack of interoperability to share CBRN tools and information. Then, NATO MSG-096 (Consequence/Incident Management for Coalition Operations) investigated how CAX simulation systems can be developed to support enhanced modelling of CBR scenarios relevant to NATO operations to provide training benefit. A key objective of this group was to provide recommendations on how CAX simulation systems interoperate with specialised CBR simulation systems through common NATO standards. Among these recommendations, the most relevant were the following, related mainly to interoperability:

– CBR Executable Scenario Description: the Military Scenario Definition Language (MSDL) to define the Executable Scenario description should be updated to include CBR content.
– CBR M&S Interoperability: a CBR Federate Object Model (FOM) was developed and integrated within the NATO Education and Training Network (NETN) FOM as the recommended Information Exchange Data-Model. The IEEE 1278 Distributed Interactive Simulation (DIS) standard was identified as an alternative approach but likewise does not have any CBR capability and would need to be extended to include a CBR DIS enumeration set within a CBR Protocol Data Unit (PDU).

Following these recommendations, a CBR Task Team started within NATO MSG-106 to follow up on the recommendations of NATO MSG-096.

A CBR FOM module was developed by DSTL and Riskaware Ltd. to allow CBR modelling information to be exchanged within HLA federations. This built upon previous work undertaken by Dstl and QinetiQ to develop an Atmospheric Dispersion Base Object Model (BOM). The CBR FOM Module covers a description of the initial CBR event through to the effects of that CBR event. The CBR FOM module can be broken down into the following sections:

– Source release modelling: Enables the transfer of information regarding a CBR release i.e. the source term parameters for an instantaneous chemical release (such as the mass and release location).
– Detector modelling: Enables the transfer of information required to perform detector modelling and the outputs from a detector model i.e. the CBR materials that a detector can detect or a detector's alarm state.
– Effects modelling: enables the transfer of information that is output from a CBR effects model i.e. the exposure data for a human or contamination status of a platform.
– Protective measure modelling: enables the transfer of information required to perform the modelling of protective measures as well as the output of the models i.e. individual and collective protective posture and protection factors.
– Hazard area information: enables the transfer of contour information for a CBR release i.e. the contours of the concentration, deposition and dosage of a CBR release as calculated by a dispersion model.

Starting from a different point of view, also MSG-147 worked more recently on CBRN related M&S activities. MSG- 147 is dedicated to develop and test a concept for M&S decision-making support for Crisis Disaster Management & Climate Change Implications. Part of these activities were triggered by a CBRN incident. The project is described in ref. [7] and NATO internal documents.

Specifically, a good number of testing to connect through HLA different tools also involving CBRN information were performed along three years. The main objective was to give the leadership of all tools to a specific tool, called Disaster Management (DM) and developed at NATO Crisis Management and Disaster Response Centre of Excellence (CMDR COE). The M&S tools involved were HPAC (Hazard Prediction and Assessment Capability (HPAC) - Ref. [9]), VBS3 (Ref. [10]), MASA SWORD (Ref. [11]), JCATS (Ref. [12]), ST-CRISOM (Ref. [13]), EMERSIM (Ref. [14]), EDMSIM (Ref. [15]), MILSIM (Ref. [16]), COBRA (Ref. [17]) , KORA (Ref. [18]) and ARCHARIA (ref. [19]). For each tool, a description is provided as well as the

characteristics and drawbacks emerged during testing which determined also recommendations.

All These experimental activities are described in details in ref. from [4] to [7].

In the USA, a specific project was developed to integrate as much CBRN specific information as possible in their CBRN M&S layer. Compared to the other testing activities, they stressed less their system for interoperability, yet it was interoperable, but they were able to include specific develop tools to take into account filter duration, the effect of weather conditions on agents and many others detailed considerations. The CBRN agent diffusion was simulated by HPAC (Hazard Prediction and Assessment Capability), while the CGF M&S Tool was OneSaf. Details are not available for NATO partners yet, but general information can be found in ref [8] where the system of system developed is described from the procurement perspective.

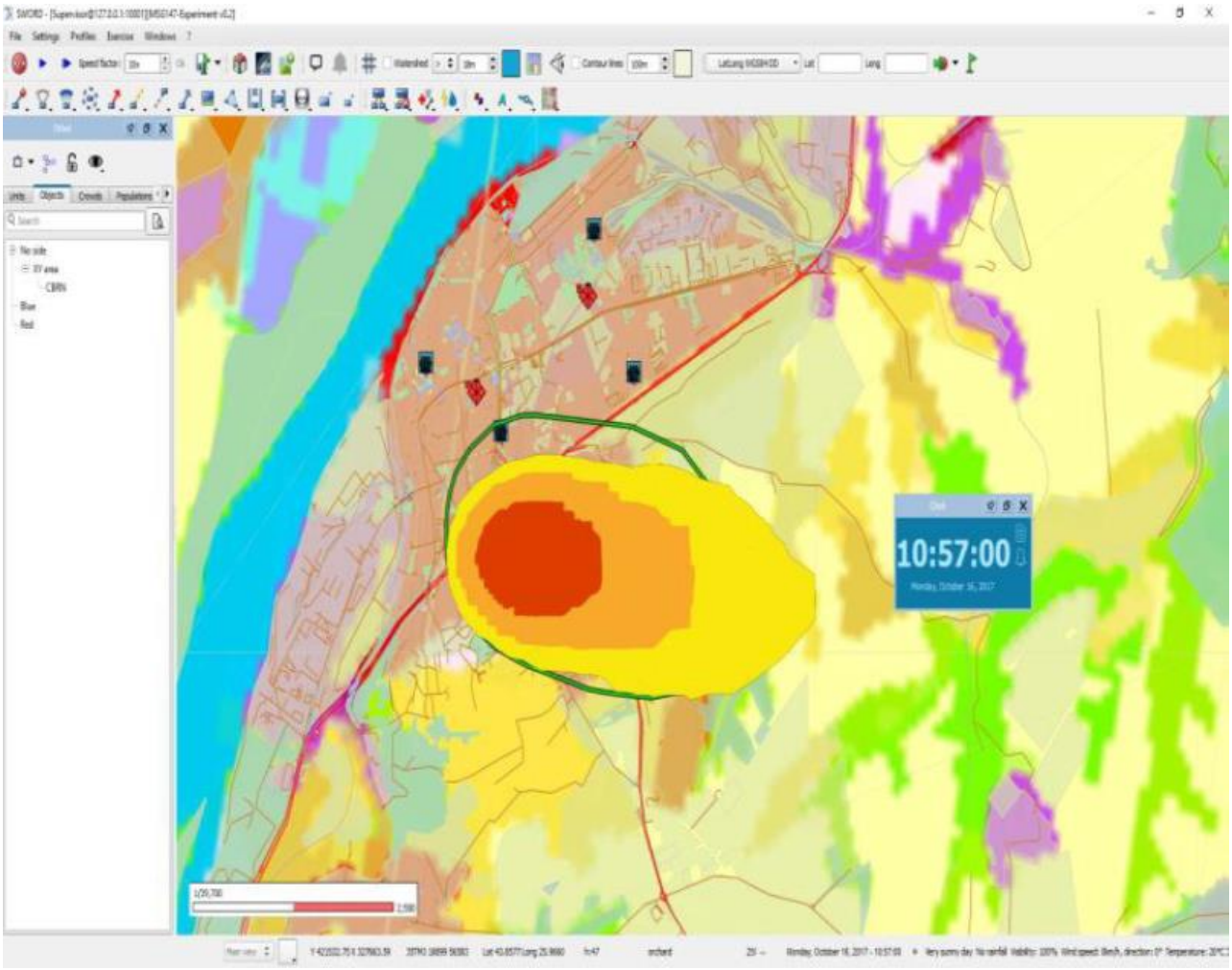


Figure 1. CBRN plume produced by HPAC projected within SWORD (From [4]).

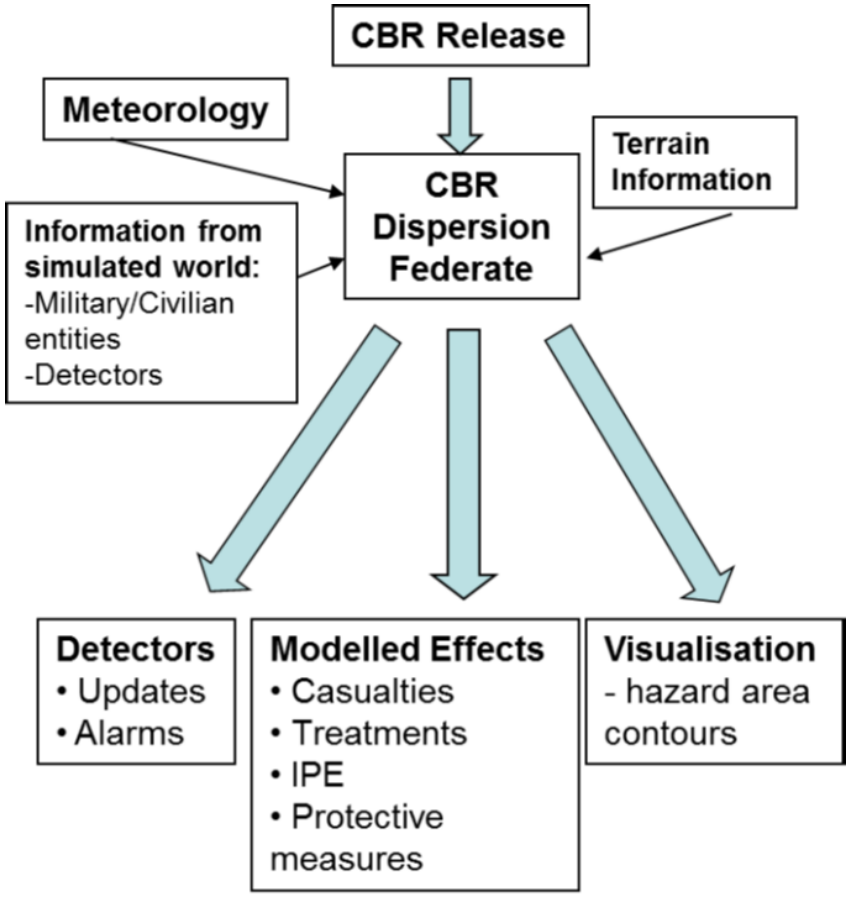


Figure 2. CBRN FOM module overview (From [5]).

4 Gap Analysis

The existing capabilities, despite experimental, should be compared to what could be provided by a CBRN layer (nice to have), described in paragraph 2. After that, the list of capabilities were reported on the left side and comment on the availabilities, as far as possible now, on the right side of the following table:

Capability	**Gap Analysis (mainly military perspective)**
Provide real-time access and automated reach-back to plume modelling capabilities with the incorporation of real-time weather data.	Achieved at experimental level.
Establish situational awareness of current/forecast plume transport direction and hazard areas.	Achieved at experimental level, but not real time. Projection of information in real time to provide assessment for military application could be critical. Need testing to verify current operations application.
Support contingency planning, damage assessment, development of response strategies, and consequence management as well as the development of protective action guides/ recommendations to deal with the short and long-term health and other adverse effects of a hazardous release.	Support is possible, but there is a clear lack of connection with software used to calculate long-term effects. Specific bridges need to be developed within the CBRN layer.

Estimate potential damages, casualties, illnesses, fatalities. The calculation could be assigned to specific tools inserted within the Architecture.	Potentially possible, the level of accuracy strongly dependent on the SW used. Need to develop a platform that can potentially include assessment of situation if personnel wear or not wear IPE. Need to use realistic database to calculate the effect of the agent and the time correlated beneficial of IPE (filters duration)
Estimate emergency assistance requirements.	Not essential. Future assessment.
Project areas where buildings, land, agricultural crops, bodies of water, and other man-made or natural resources are or will be contaminated.	Possible.
Select locations for incident command sites, decontamination facilities, sheltering, and evacuation areas.	Possible, with human contribution. Artificial Intelligence could be an added value.
Determine emergency response and health services facilities impacted by the release.	Possible.
Make shelter-in-place, evacuation, and personal protective equipment use decisions.	Support human to take decision. Artificial Intelligence could be an added value.
Identify safe approach and evacuation routes.	Support human to take decision. Artificial Intelligence could be an added value.
Guide field measurement and aerial sampling teams.	Support human to take decision. Artificial Intelligence could be an added value.
Determine radiological monitoring requirements.	Possible.
Estimate the source amounts and locations of unknown releases.	Not useful for military applications.
Obtain information for communications with the public to allay concerns.	Not useful for military applications.
Support post-event analysis for exercises and actual incidents.	Possible, using some post analysis tool embedded in some tools (e.g. MASA SWORD). Improvement could be achieved using Artificial Intelligence.

Table 1: Gap analysis on the required capabilities.

The next table provides a first gap analysis on technical requirements:

Technical requirement	**Gap analysis**
Predict the initial direction, travel, and dispersion of a plume over time from a single or multiple sources taking into account the type of source, material/chemical properties, release location, weather conditions, terrain, urban areas, and other man-made structures.	Possible (e.g. HPAC)
Predict the concentration of the chemical or biological agent within the plume and flow through drainage areas over time.	Possible (e.g. HPAC)

Estimate deposition and contamination levels for air, water, ground, and building surfaces.	Possible (e.g. HPAC)
Identify exposed population and predict exposure levels over time.	Possible (e.g. HPAC)
Identify the time when the sensors placed in the area of interest will be triggered following the release of the plume.	Possible (e.g. HPAC)
Provide for reverse simulations to estimate unknown source amounts, probable release locations, and support event reconstruction.	Not useful for military applications.
Provide capabilities to refine simulations based on field measurements and other sensor data.	To be investigated.
Support a number of different established problems, models, representations, and techniques including chemical, biological, radiological, nuclear, and explosives (CBRNE) source characterizations, Gaussian-plumes, dense gas dispersion physics, boundary layer meteorology, atmospheric turbulence, urban flow and dispersion, high altitude dispersion, time integrated dosages, inverse modeling and event reconstruction.	Need further investigation, but it is not essential for military application. It could be valued for specific application integrating several expert systems, e.g. CD&E applications.
Automate the utilization of sensor field measurements to estimate source terms and optimize predictions.	Useful for CBRN specialist troops. To be investigated.
Couple sensor data and simulations via Bayesian inference, stochastic sampling, and optimization methods.	Useful for CBRN specialist troops. To be investigated.
Perform backwards analyses to determine probabilistic distribution of unknown source characteristics.	Not useful for military applications.
Generate optimal and probabilistic forward plume model predictions.	Possible (e.g. HPAC)
Use Markov chain sampling to determine probabilistic source locations based on sensor readings, Green's function methodology (heat conduction and diffusion), fate and transport models.	Useful for CBRN specialist troops. To be investigated.
Provide source characterization models for explosive dispersal devices that predict airborne fractions and particle-size distribution.	Useful for CBRN specialist troops. To be investigated.
Provide fast-running empirical urban models and high-resolution building-scale computational fluid dynamics models use finite element modelling (FEM) techniques.	Useful for CBRN specialist troops. To be investigated.
Support vector and raster representations of geography, buildings, and other structures.	Possible.
Support a range of different grid resolutions, e.g., 30 meter, 100 meter, 1 kilometre, and 10 kilometre.	Possible.
Model indoor exposure levels due to the effects of building leakiness, i.e., outdoor plume air concentration versus corresponding indoor air concentration.	Possible using civil application SW.
Support the integration and/or distributed execution of interrelated models including dispersion, weather, exposure and hazard effects, watershed flows.	Possible for military tools, to be investigated for specialized tools.
Support various release mechanisms including explosions, fires, volcanic eruptions, gas cylinders, sprayers, manual methods, tank ruptures, and building collapses.	At least partially possible (e.g. HPAC). Further analysis needed.
Support micro and meso-scale forecasts (10 km).	To be evaluated.
Model radiation effects including fallout, wet deposition hotspots, ground shine, cloud shine, and inhalation doses.	Possible (e.g. HPAC): Military relevance to be assessed

Identify regions where the exposed population will experience life threatening, serious long lasting, or notable discomfort effects.	Possible.

Table 2: Gap analysis on the technical requirements.

Other important pieces of information to be taken into account in our gap analysis are reported in the following table:

Constrain on data input	**Gap analysis (mainly military perspective)**
Meteorological data: observed and forecast weather conditions that may affect a plume including wind speed, direction, and precipitation	Possible.
Plume release mechanisms and their attributes: explosions, fires, compressed gas cylinders, tank ruptures, and manual release of powders	Possible (e.g. HPAC).
Specifications of characteristics of an explosive release: detonation point, explosive source characteristics (particle size distribution and spatial distribution of mass from surface to several hundred meters above ground)	At least partially possible (e.g. HPAC). Further analysis needed.
Hazardous agent characteristics including form (gas, liquid, or powder), chemical properties, particle size and weight distributions, cohesion, and lethality	At least partially possible (e.g. HPAC). Further analysis needed.
Specification of the incident area including location of source, terrain, and buildings	Possible.
Demographics data – population location, density, and attributes by time of day	Technically possible, but problem could arise with data source.
Setup requirements	**Gap analysis (mainly military perspective)**
Provide capabilities to configure simulation runs with specific release incident parameters, weather conditions, and geographic regions.	Possible.
Provide a capability for modifying of key release parameters including location of source, agent characteristics, and location of sensors.	Possible.
Generate graphical views of plume dispersion over a 2D or 3D representation of area of interest.	At least partially possible (e.g. HPAC). Further analysis needed.
Provide user control mechanisms that effect rapid execution/playback of simulation runs to move forward and back to desired points in time.	Possible.
Use various representation schemes to display release effects including chemical concentration, radiation intensity, toxicity, lethality, and exposure levels, e.g., colours, shading, contour lines.	Possible.
Provide interfaces to generate still image and video files that can be used to transfer results for viewing or playback using other software tools.	At least partially possible (e.g. HPAC). Further analysis needed.

Considerations on performance	**Gap analysis (mainly military perspective)**
Support fast running local models that generate predictions in 5-15 minutes.	Possible.
Provide for updates from real time meteorological databases and observations.	Possible.
Share model predictions with other software applications, e.g., incident management applications.	Possible.

Table 3: Gap analysis on constrain on data input, setup requirements, consideration on performance.

The following table is devoted to perform a gap analysis on the capability more strictly related to military applications:

Capability more related to military applications	**Gap analysis (mainly military perspective)**
Determine where and when military personnel or civil servant should don IPE;	Existing with a certain level of accuracy. To be verified and eventually implemented, using existing tools or developing specific tools, with high accuracy.
Determine where and when military personnel or civil servant should not don IPE anymore;	Existing with a certain level of accuracy. To be verified and eventually implemented, using existing tools or developing specific tools, with high accuracy.
Determine mask's filter duration as a function of the concentration and time of exposure (integral C(t)dt > Filter saturation);	Existing with a certain level of accuracy. To be verified and eventually implemented, using existing tools or developing specific tools, with high accuracy.
Determine where and when Vehicle should employ CBRN Filtration Systems;	Not available
Determine where and when Vehicle should stop employing CBRN Filtration Systems;	Not available
Determine vehicle's filter duration as a function of the concentration and time of exposure (integral C(t)dt > Filter saturation);	Not available
Determine the best route (as a function of speed, also) to go from a starting point to an ending point avoiding as much CBRN contamination as possible;	Not available
Determine the burden and operativity limitation for personnel, vehicle or other equipment during CBRN exposure (it exist to some extend); consequently, determine the effect on operation (training, exercise, mission rehearsal) so as to assess the risk balance;	Not available
Determine deaths and casualties if CBRN procedures are not well followed during virtual exercise (e.g. IPE don or not don, filters durations, filtration systems employed, etc.).	Not available

Determine where to send SIBCRA Teams, UAV, UGV or any other useful tools to detect the threat, sample soil, water or gas, so as to confirm the predicted contaminated area and delimitate the exact contour;	Not available
Use the information provided by detectors and sampling analysis to adjust M&S input so as increase the reliability of prediction on contaminated areas.	Not available
Determine weather effects on CBRN Agents, such as degradation of chemical compounds due to the temperature, direct sunlight, water, etc... or the survivability of spores, viruses and bacteria.	Not available

Table 4: Gap analysis on military capabilities.

5 Next Steps

In the next future, we will try to revitalize the architecture organized during the MSG-147 possibly integrating also, what was done within MSG-126. The idea is not only to organize other testing activities, bringing together as much tools and databases as possible, but also to check point by point all the elements determined in the Gap analysis provided in the previous paragraph. The identified solutions should then be fixed in the architecture and the associated documents. Whenever a solution for a specific gap has not been identified with the available tools, a tentative to fill the gap will be performed programming a custom solution (e.g. Matlab, C, specific API to integrate SWs or database). If it is not possible to develop a solution with the available resources, a way ahead will be identified to start a procurement process to acquire the SW tool development.

In the long term perspectives, the architecture, with all databases and SW included, will be shared within NATO Community of Interest for testing, verification and validation by Subject Matter Experts (and to start being a useful system), eventually employing the capability provided by current technologies to share resources remotely (Modelling and Simulation as a Service – MSaaS approach).

6 Conclusion and Perspectives

CBRN and M&S should be integrated to fully exploit, within their potential in the military domain, using ideas that have already been developed and explore how to improve or shape for different military requirements. Nevertheless, there is still the need to integrate all the activities in one-concept, bringing all the stake-holders around the same table, with the objective to further develop a comprehensive CBRN Layer, taking into account any missing capabilities and sharing the existing resources to finally achieve a tool usable within the NATO Community of Interest. The first step of this process could be to activate a clear procedure to have access and the possibility to explore new applications into the architecture developed within MSG-147 in the CMDR COE. This will facilitate a way ahead to fill the gap, involving as many stakeholders as possible in the project. The involvement of the USA in this effort would raise the level of the project considering their comprehensive approach in this field.

A final analysis of each available capability, and the system as a whole, should be performed to clearly identify further capabilities to be included or developed while also addressing any interoperability issues.

Testing each capability and the system for verification and validation purposes should be planned as well.

Finally, availability and use of the system from a wide Community of Interest needs to be considered in order to have the maximum benefit for NATO and Nations and to continue improving the system itself through suggestion and contribution from users and developers. A general layout of the CBRN layer is provided in the following picture.

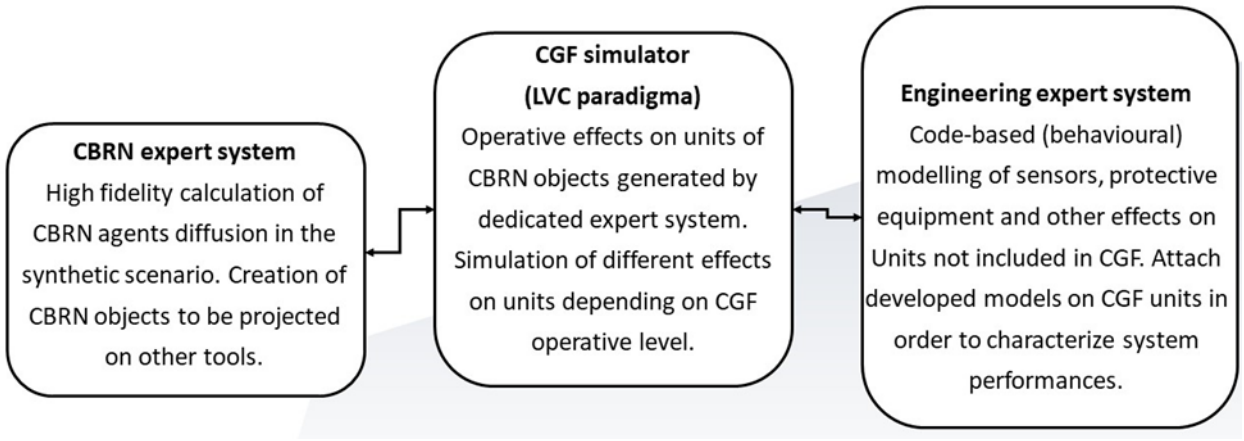


Figure 3: General Layout of a CBRN layer.

References

[1] Charles McLean, Y. Tina Lee, Dr. Sanjay Jain, Dr. Charles Hutchings, *Modeling and Simulation of Hazardous Material Releases for Homeland Security Applications.* – National Institute of Standards and Technology - NISTIR 7786, 2011

[2] NATO STANAG 2499 "*The effect of wearing CBRN individual protection equipment on individual and unit performance during military operations*" – ATP-65(B)

[3] NATO STANAG 4625 "*Assessment of effect levels of classical chemical warfare agents applied to the skin to be used in the design of protective equipment*" – AEP 52

[4] Lt Col Walter David et al., *Crisis Decision-Making with M&S Support in Complex Urban Environments*, I/ITSEC 2018, from https://www.researchgate.net/publication/331044317_Crisis_Decision-Making_with_MS_Support_in_Complex_Urban_Environments

[5] Jon Lloyd, Nathan Newton and Richard Perkins, *A Chemical, Biological and Radiological Modelling Capability to Support Acquisition Advice and Re-use as a Common Cross-Domain Capability.,* DSTL – UK, - STO-MP-MSG-126, from https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-126/MP-MSG-126-09.pdf

[6] Jon Lloyd, Nathan Newton, Jose Ruiz, David Desert, Antony Hubervic, Lennart Olsson and Russell Mills, A Common Chemical, Biological & Radiological modelling capability: UK and NATO HLA-Evolved experimentation. from https://www.sisostds.org/DesktopModules/Bring2mind/DMX/API/Entries/Download?Command=Core_Download&EntryId=42367&PortalId=0&TabId=105

[7] Orlin NIKOLOV, M&S support for Crisis and Disaster Management Processes and Climate Change implications, https://drmkc.jrc.ec.europa.eu/Portals/0/Partnerships/Seminars/3_Scientific_Seminar_DRMKC/Presentations/session_4b/pdf/3_orlin_nikolov-

m_and_s_support_for_crisis_and_disaster_management_processes_and_climate_change_implications.pdf

[8] Ms. Gail Cayce-Adams and Mr. Michael Kierzewski, JPEO CBRND develops a new concept to better manage its portfolio, from https://asc.army.mil/web/news-alt-jas18-analytical-framework/

[9] Hazard Prediction and Assessment Capability (HPAC), by Defense Threat Reduction Agency

[10] VBS3, from https://bisimulations.com/sites/default/files/data_sheets/bisim_product_flyers_june2020_vbs3.pdf

[11] MASA SWORD, from https://www.masasim.com/en/sword

[12] JCATS from https://computing.llnl.gov/projects/jcats#:~:text=Originally%20designed%20for%20the%20U.S.,Department%20of%20Homeland%20Security%20programs.

[13] CRISOM, from http://www.liophant.org/projects/st_crisom.html

[14] EMERSIM, from https://simofun.com/emersim

[15] EDMSIM, from https://www.c4itrgtech.com/2021/02/04/edmsim-emergency-and-disaster-management-simulation/

[16] MILSIM from https://www.c4itrgtech.com/products/

[17]COBRA, from https://cobrasimulation.com

[18] KORA, from https://www.iabg.de/fileadmin/media/Broschueren/DS/DS_KORA_en.pdf

[19] ARCHARIA, from https://www.mscoe.org/nato-ms-coe-archaria/

Technical Report for AI/ML M&S Integration in Support of Decision Making

LTC Piergiorgio Ventura (ITA Army)
Concept Development Section Chief - NATO M&S CoE
mscoe.cde02@smd.difesa.it

Ref.: NATO M&S CoE n. 0002/2022 dated 02 November 2022.

1 Introduction

In 2022, the M&S CoE provided support to the Italian MoD Innovation Office in order to determine the technical specification required to develop a system capable of integrating AI (Artificial Intelligence) / ML (Machine Learning) with M&S (Modelling and Simulation) in order to support the decision-making process.

The M&S CoE delivered the technical document with the letter in reference.

The idea and the technical elements beneficial to explore the concept were further developed in 2023. Some information was released during specific meetings in order to provide guidance for the procurement phase. This document provide the general information useful for developing the project.

2 General Concept

Artificial intelligence (AI) is an emerging technology that has been progressively developing in the last period. In particular, the branch of machine learning (ML) is finding substantial use within digitized contexts, favouring the development of innovative concepts and solutions in the IT sector. In a context of emerging technologies exploration, the integration of AI, including any possible technical solution such as Deep Learning and Supervised Learning, with Modelling & Simulation (M&S) assumes a fundamental technical and operational value for the benefit of military operations and concept / capability development, with the aim of supporting the decision-making process.

In this context, it should be noted that the fundamental peculiarity inherent in the main AI / ML applications lies in the deductive programming mode, in contrast to conditional algorithms, which are structured on an inductive logic. The aforementioned deductive logic represents the foundation of the initial concept, or rather an adequate integration of the AI / ML with the M&S.

In particular, the proposed integration provides an architecture based on the bi-directional connection between a neural network and M&S tools, in order to extend the peculiarities and results provided by a synthetic environment with algorithms based on deductive logic. The technological coherence of the proposed integration is essentially based on the main characteristics of the computational processes put in place by a constructive/virtual simulator, which refer to stochastic results. The computational engine of the main simulators is based on databases (physical and / or behavioural) that define the models of the units.

The final result would be an integrated system able to "predict" the best behaviour (Course of Action) in a specific situation, based on its experience in similar situation, to be applied for decision making support within training activities or, ideally, even for real operations, at least in the planning phase.

3 Architecture

The system architecture will be based on the following components:

– M&S computer generated forces tool(s) - CGF: Used to 'play' military actions to be run several times, changing parameters to train the network and then to evaluate a new Course of Action. First test will be performed with MASA SWORD because of its high flexibility and is possible to use it with High Level Architecture (HLA) and Application Protocol Interface - API (C#

& Python). Further testing with JTLS and additional simulators, will be performed in the following blocks as soon as feasible. The M&S CoE owned platform WISDOM will also be used to visualize results and to enhance information sharing.

– AI specific tool: SW and HW used to run the specific application to train the network and used to evaluate Course of Action. MATLAB would be preferable considering the possibility to address specific problem with the support and the warranties of official developers, compared to free software.

– M&S expert system(s): Used to run simulations that provide specific information to the system: EMSO, CBRN, weather condition, terrain, etc.. These systems should be chosen as a function of use case: STK – MATLAB for EMSO applications and HPAC, ALOHA, CBRN Analysis, HOTSPOT or other diffusion tools for CBRN applications.

– Database(s): Used to provide external source of information about terrain, weapon systems, logistics, effect of environment on units (e.g. CBRN agent), etc.. It can be used to store "experience" from AI as well. This is a critical point to be addressed also with the help of other components experts/developers.

All components will be enabled to share information with HLA, as a first option, and API as an alternative one, in order to allow complex exchanges of information such as those determined by the loop involving CGF and AI tools. In order to fix the main information and determine the structure, specific software socket requirements have been identified to allow MASA SWORD sharing the most significant pieces of information with the future AI tools. These requirements are described in the following paragraph, whilst the SW developed by the company is under CDE Branch custodianship. Most of the knowledge could also be applied for other CGF tools.

4 Aim of the MASA SWORD Socket

The idea is to create a way to exchange data between the M&S tool (socket) and the AI system (Spine). The best solution seems to be the creation of a client script, which exploits SWORD API (Application Programming Interfaces) in C#, able to read and write simulation data from an exercise. The exchange of information is built in two macro-areas: data reading and data writing, in order to train a neural network for classification purpose and to provide deductive results. Only the data-reading phase has been conceptualized and, therefore, it will be described in the next paragraph.

5 Structure of the MASA SWORD Socket

A root folder should be created by client script for each exercise. In this folder, it is expected to find the so-called common files, which can affect all forces' factions (terrain.xml, weather.xml, physical.xml).

Moreover, it is expected to find a folder created by client script for each automata. In the automata folder, it is expected to find a folder created by client script for each units, containing the information of the unit itself and its equipment.

At simulation tick zero (initialization phase), it is expected to find an xml formatted file with the following fields:

- Time (tick)
- Diplomacy
- Hierarchy
- Status (strength)
- Unit type
- DIS type
- Properties:
  - Fuel
  - Ammunition
  - Sensors (type and punctual probability of detection)
  - Weapons (type and punctual probability of detection)
  - Crew (dead/injuries)
  - Human factor (tired, veterans, etc.)

- Interactions
- Reports
- Mission
- Posture
- Terrain layer (only for land unit) -> modifiers (useful for having sensors and weapons probability of detection)

After the tick zero initialization file, all the field of the unit should be formatted in the xml file. To avoid a huge amount of data during the polling at each simulation time, it is expected to create xml file containing only the units' updates, in the same units' folder.

In this root folder, it is expected to find the results' folder created by the client script containing the COAs data in csv format (time vs value). This piece of information will be used by neural network for classification.

6 Scenario Generation

A different and complementary application that could be studied in the future and applied also to Wargaming, is the possibility to automatically generate scenarios, including ORBAT, after proper training with already developed ones. This solution could be used for:

- Training sessions;
- Operational scenarios fed with real data (i.e.: open source about countries involved, intelligence, etc.);
- Conflicts simulations among different parties feeding the other AI-driven M&S.

MATLAB have developed a specific set of tools that are used for building projects through generative AI. It seems to be a good starting point for this application to be investigated in the future.

7 Conclusion

Within the system architecture, the M&S Tool socket and the complementary AI tool spine, will be developed to initially test their effectiveness using the available software and a standard PC with full Matlab license installed. Preliminary tests, using a simplified version of the training structure, will be conducted to verify its results. Afterward, when the whole framework will be available, the SW package will train the neural network and develop the desired decision making support tool.

The project will also include a proof of concept on new scenarios and ORBATs generation, finalized and delivered with a specific technical document.

Using MATLAB, able of creating from scratch new SW components project using generative AI, the proof of concept will be validated through testing of the new scenarios and ORBATs, employing limited amount of data, for final capability development.

WISDOM: The Development of a Wargaming Platform and its System Architecture

Lt.Col. Federico Mazzone (ITA Army) and other authors

NATO M&S CoE

Abstract

Over the years the M&S COE has developed, together with the support of the industry, the Wargaming Interactive Scenario Digital Overlay Model (WISDOM), a software tool for the configuration of geographical scenarios. This platform is particularly suitable to carry out wargaming activities and is aimed at those who need to carry out education & training activities, experimentation, AAR or preparation for real missions, both in the military and civil context.

The WISDOM portal allows system administrators to configure many different aspects of the platform and therefore create new scenarios based on real requirements. Geographical scenarios consist in selecting and organizing the data contained in the geographic database into groups and subgroups depending on how they should be displayed on the map, as well as the configuration of the various spatial analysis and management tools.

The portal, once configured, allows you to explore, through interactive maps, the geographical information of the scenario and through analysis tools, to extrapolate useful information for the decision-making process.

This platform is scalable, which means it is designed to allow the addition of new configuration parameters to continuously expand its available functionality. Additional views can be added beyond those currently available through appropriate add-ons. A 3D viewer and a representation of the scenario using vertical scrolling story maps are available and it is also fully developed with open-source systems. WISDOM platform has been succesfully used so far in various different activities like the Wargaming Initiative for NATO (WIN) 2022 and 2023 edition, and in other events and working groups.

Aim

The aim of this presentation is to provide a quick overview of M&S COE wargaming platform (WISDOM).

1 Introduction

The NATO Modelling & Simulation Centre of Excellence (M&S COE) has developed the Wargaming Interactive Scenario Digital Overlay Model (WISDOM), available to support wargaming activities. Is has been developed on the basis of past experiences the M&S COE gained through past requests for support. Several requests required a digitalized scenario able to support the wargaming activity. All scenario were different and tailored to the aim and objectives of the single event. But, all demanded the same set of functionalities like a virtual environment, layered information, task organization, wargaming support (vignettes, turns and teams), distributed execution option, storybook, simulation interface, etc.

All those functionalities are already developed and available on WISDOM. The information about the specific scenario, like maps and other data, can be organized in an activity related section on WISDOM. Scenario from past activities are also

available and can be reused by tailoring for other wargames

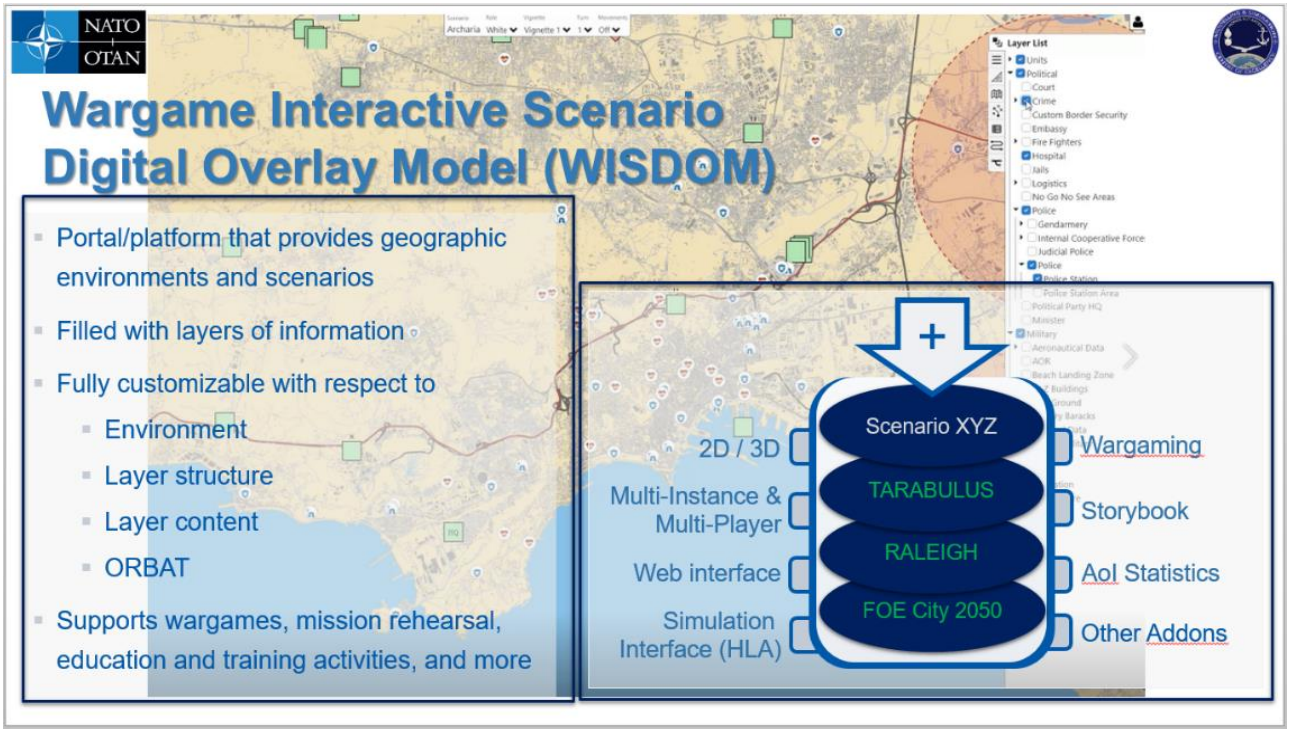


Figure 1: Wargame Interactive Scenario Digital Overlay Model (WISDOM)

In addition, there are several scenarios and geographic environments available on WISDOM from past supported activities. However, they are not easily accessible, as they require the reading of several pages of scenario documents to understand the background. Although the M&S COE has the need to introduce WISDOM to new M&S COE personnel and potential users, this requires an effortlessly understandable and clear scenario in order to concentrate on WISDOM itself rather than questioning the scenario. Additionally, wargaming is included in M&S COE courses, and table top wargames are played to practice the idea of wargaming.

As we have experienced during the pandemic situation, where the courses were conducted on-line, there were not scenario available that could be used like before during the in-person courses. These are some reasons that had triggered the idea to develop a new lightweight scenario and implement it on WISDOM. It could also be used to explore additional technical solutions like wargaming and M&S integration.

2 Scenario Design and Development

The main focus of the M&S COE in the wargaming area is the support of activities with M&S means. Therefore, the M&S COE personnel have gained some knowledge about scenario design and development. This is enabling the M&S COE to translate the wargaming requirements into M&S requirements, which is key in order to provide the right solution. Anyway, the decision was to choose an already existing scenario rather than designing and developing a new one.

Normally a wargame has to fulfill an operational purpose with a well-defined aims and objectives. As introduced in the former section, the purposes of the scenario does not follow operational needs. The focus is instead teaching, conceptually the general design of a wargaming event. This means

the scenario theme is not so important as long as it is coherent and the audience is not questioning the scenario itself. The most important aspect of the desired scenario is its simplicity in order to enable the user to understand the mechanics more quickly. That was why the decision was made to exploit the "Enhanced LUNA Warrior" scenario.

The game is designed as a helpful tool able to stimulate decisions for the training of flight planning of manned and unmanned aircraft (UAV). The BLUE Team plays as an aircraft operator of an unmanned aicraft during a reconnaissance mission. The RED Team is acting as a terrorist group that tries to destroy a bridge in norther Afghanistan. Intelligence reports possible terrorist's home bases. BLUE tries to detect the terrorist group before it reaches their target. The map is divided into hexagons. No fly zones restrict the movement of the UAV. The UAV itself can move up to two hexagons per turn and the sensor covers all adjacent hexagons. RED can move one hexagon per turn and has no further movement restrictions. The adjudication is done by a WHITE Cell. All in all it is a very basic scenario. Nevertheless, subject matter experts validated it and approved the scenario to be valuable for the purpose it is designed for.

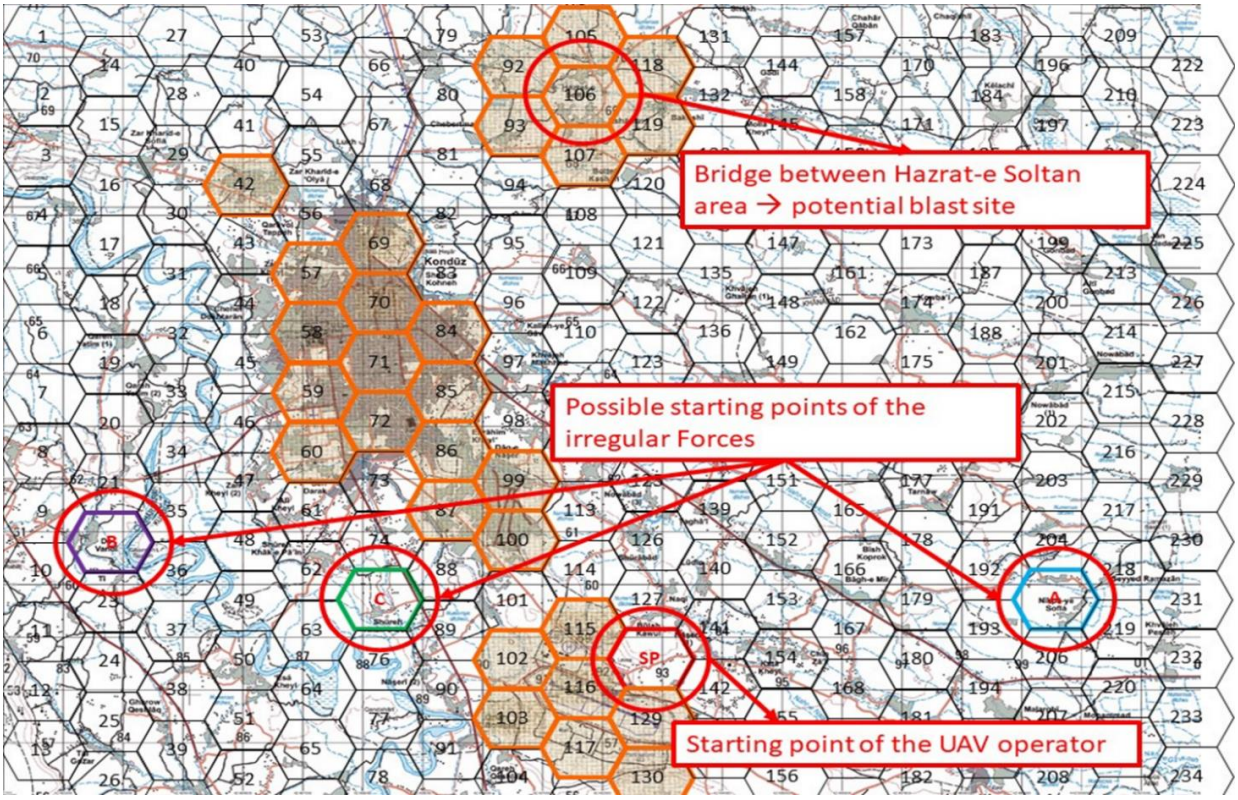


Figure 2: Enhanced LUNA Warrior table top game scenario map

3 Implementation

The scenario we implemented on WISDOM was the same as the table top game. Nevertheless, some decisions had to be taken in order to fit it to the technical platform. First of all, the digital platform and the low level tactical scenario offers the opportunity to automate the adjudication process. However, the M&S COE normally supports wargame activities at the operational level with adjudication by a WHITE cell. That is why the game is still played with three teams. To support the WHITE team, and to give it some advantage from the digital solution, automated movement restrictions and detection evaluation have been implemented to be chosen optionally. Another change to the original table top game is the map. Instead of using the hexagons we took advantage of

the already available coordinate system on WISDOM, which also gives a much better idea of the geographical environment.

The implementation phase was not only throught to make the scenario available on WISDOM, but also to educate and train new M&S COE personnel on the technical aspects of the platform. The implementation was possible thanks to support of the industry.

The M&S COE has been closely worked together with partners from industry and academia for a long time and this close cooperation is one of the key factors for the succesful development of WISDOM.

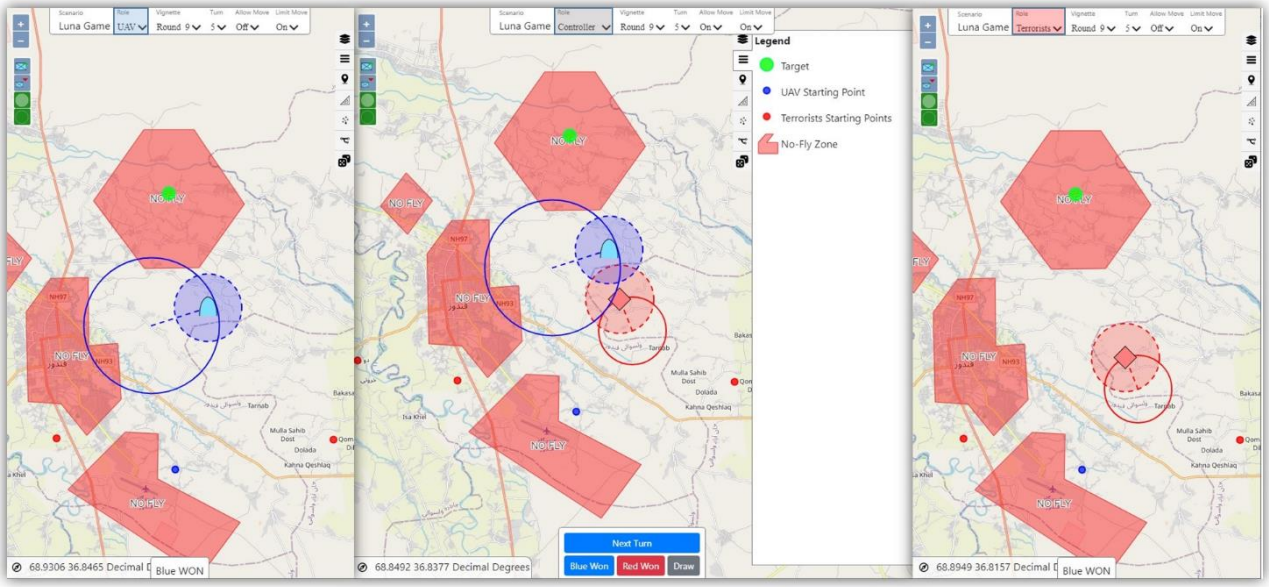


Figure 3: Enhanced LUNA Warrior scenario on WISDOM with BLUE, WHITE and RED team perspective

4 New Scenario

The new scenario on WISDOM has already been proven to be valuable for the described purpose in the introduction section however, the M&S COE has also developed another wargame on how to utilize M&S means for wargaming activities. The intent is to use WISDOM as one model that can be used to support wargames with a focus on distribuited wargaming. The Enhanced Luna Warrior scenario is a good starting point, but it was concluded that there is a need to extend the scenario in order to implement a larger scale of complexity in the wargame. The idea of the Enhanced Luna Warrior – LUNA Sprint scenario was elevated on a larger scaled tactical scenario in the Tripoli, Libya area by using the already existing geographic enviroment called TARABULUS.

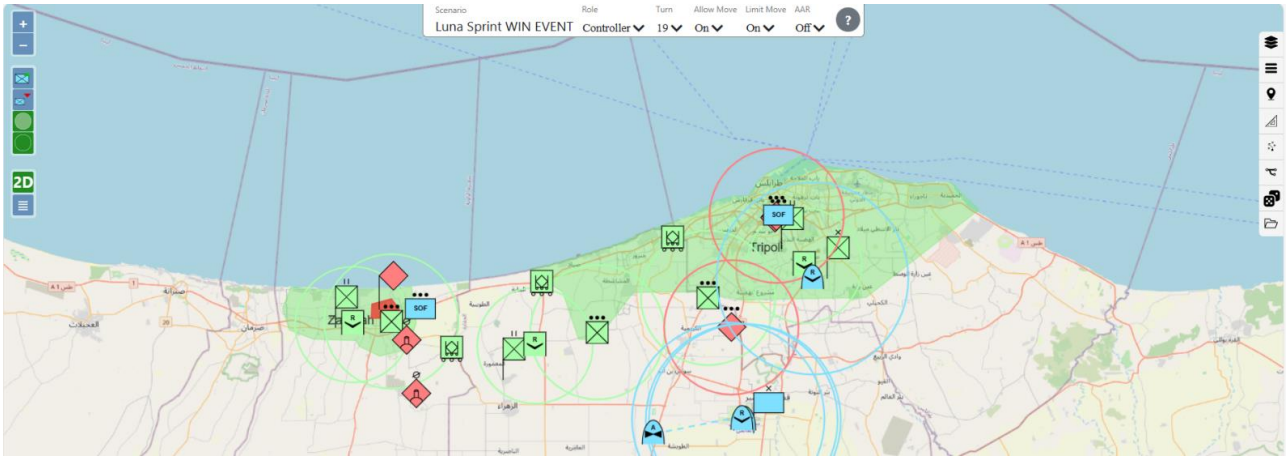


Figure 4: Enhanced LUNA Warrior scenario on WISDOM – LUNA Sprint view 1

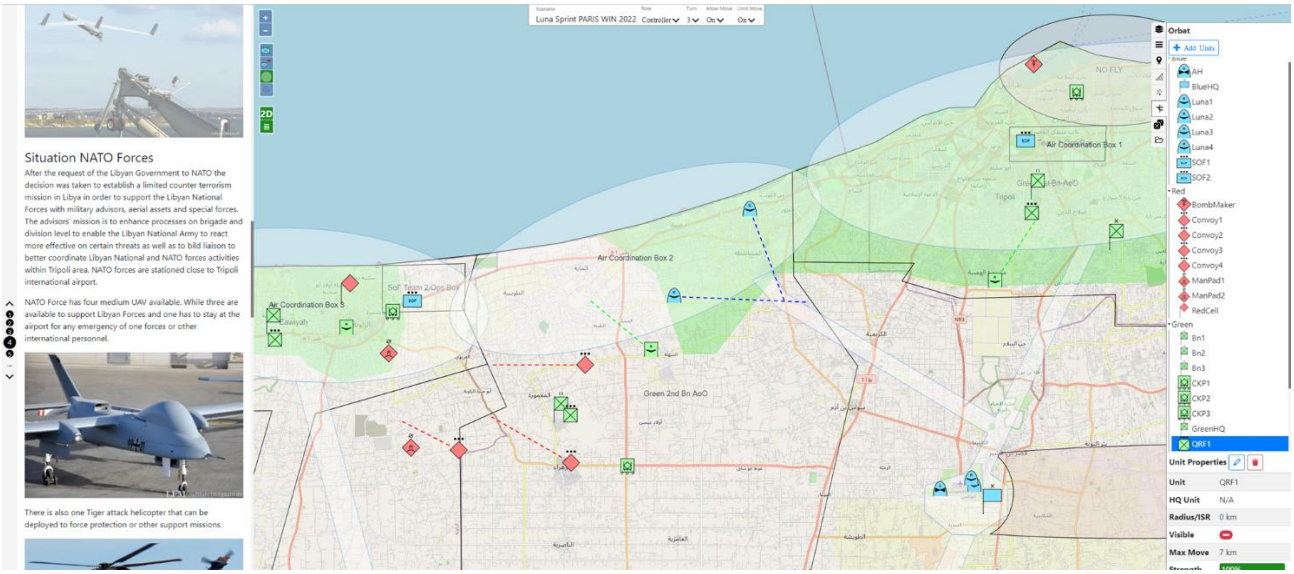


Figure 5: Enhanced LUNA Warrior scenario on WISDOM – LUNA Sprint view 2

Another part the M&S COE has investigated is the use of simulation for wargaming activities. Anyone of us will confirm that this is a very natural step. Simulation can serve different purposes in a wargaming activity. It can provide support to the adjudication phase by simulating engagements of forces on the battlefield and calculating the outcomes. Another opportunity would be to gather not only qualitative results from a wargame, but also get quantitative figures, which supports more informed decisions.

5 System Architecture

To better understand how WISDOM is implemented and how the creation of new tailored scenarios is possible, I am going to give a short overview about its System Architecture.

WISDOM uses a data model from PostGIS DataBase based on Linux. Data are created or elaborated from QGIS which is a software application able to manage spatial data. With QGIS, it is possible to edit GIS data and create a further new database for PostGIS; this database will be afterward loaded and utilized on WISDOM that is in turn based on QGIS Server.

WISDOM therefore is a GIS server platform based on WebGIS Architecture.

As opposed to ESRI VM architecture (Old Project and prototype for WISDOM), WISDOM architecture is running on just one comprehensive Virtual Machine with all the internal connection on localhost between server and database.

On the second release, WISDOM can use microservices for some applications. These microservices are isolated process from the main "Core" WISDOM Server and they can run independently from it. In this way, you can use microservices just when needed, saving hardware computational resources.

Thanks to a microservice architecture, the main "Core" WISDOM Server will run correctly even if a microservice isn't properly working (you can't use just the feature the microservice provides you). Additionally you use the architecture of container to create a more isolated environment; this is why WISDOM uses Docker to manage the microservices as containers. This architecture allows a future porting on clouding for WISDOM, easily managing the scalability of the applications.

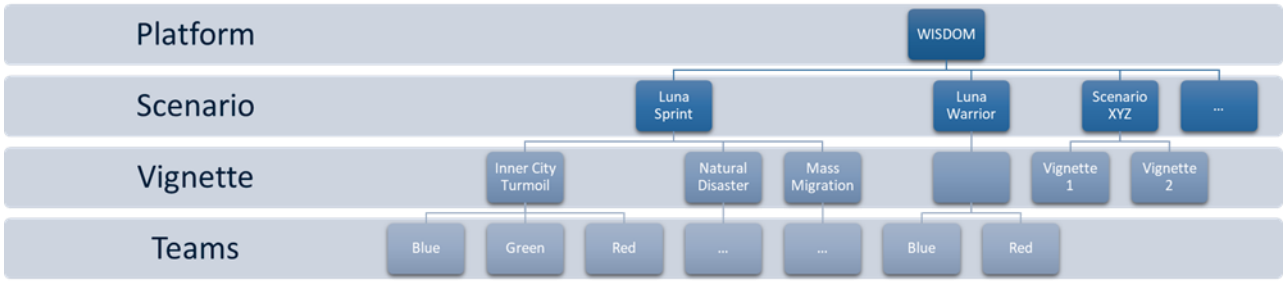


Figure 6: Architecture

6 Conclusion

This is briefly how WISDOM works and the new scenarios have already proven their usefulness for the proposed purposes. They were play tested within the Centre and used to introduce visitors to WISDOM during multiple events by M&S COE personnel.

Additionally, Enhanced Luna Warrior was utilized during the M&S Basic Course to provide the attendees with a better understanding of wargaming.

As benefit, these activities have given an enhanced understanding of scenario design and development and about the needs of wargaming experts, which leads subsequently into improved M&S solutions, with enhanced support to the purpose of the wargames.

The follow up action on wargaming and simulation is the next step on the road to an enhanced M&S support to wargaming activites. In that sense, the availability of the operational requirements is a key factor and allows to develop a proof of concept, related to real needs and validate the approach.

Part 2:

CA²X² Forum 2023

The NATO Modelling and Simulation Centre of Excellence team thanks you for participating the 2023 Forum.

The CA²X² Forum 2023

Sponsors Recognition

Main Sponsor

CALIAN

Platinum Sponsors

CUBIC LEONARDO Valkyrie ENTERPRISES

Gold Sponsors

Ansys Bohemia Interactive SIMULATIONS BV TECH

dataunitor FABRIS infodas connect more. be secure.

LOG.IN MathWorks MISSION SYSTEMS

ST Engineering PITCH

Silver Sponsors

Digivents BSI bistemi DELL Technologies TITANIUM PARTNER GMSPAZIO masa www.masagroup.net

The NATO Modelling and Simulation Centre of Excellence wishes to thank the sponsors for their contribution to this year's conference and for assisting with making it an incredible achievement.

This book contains the proceedings of NATO M&S CoE's Computer Assisted Analysis, Exercise, Experimentation annual conference held, from 3-5 October 2023 in Rome, Italy

The principal theme for the conference was:

'Modelling and Simulation as a Cross-Functional Enabler'

Through a team effort at the M&S COE we have captured the articles from the CA2X2 Forum allowing our readers to reference the great work done by some of the contributors. Please use these articles as inspiration for further collaboration and contributions to these important topics.

Thank you for the contributions to the forum,
the insightful questions and discussion to advance these topics.
For those that were unable to participate, this collection of articles will help you understand the level of expertise and professionalism that was displayed during the forum.
Enjoy.

If you wish to provide feedback, please send it to us at: info@mscoe.org.

Thank you and good reading!
The NATO Modelling and Simulation Centre of Excellence

Cryptography within Critical Infrastructure

Soenil Soebedar – Netherlands - Europe

Abstract

We have very often witnessed natural disasters wreaking havoc on physical infrastructure which inadvertently have severe impact on us both economically and physically. Giant Industries, Research Facilities, Health Facilities, Government agencies play vital role in our socio-economic life that guarantee our very existence. Any disturbances in any of these will mean destabilization of our systems. As we follow standardized guidelines of building industrial structures and ensuring physical security, it is equally important to secure our industrial devices interconnectivity. Failure to give all same critical attention will have dire consequences. Example if electricity supply is disrupted for hour, Water treatment system that supply water to homes is tempered with by unauthorized person who is on a revenge, an oil refinery plant control system, border control, payment systems that can be compromised , aviation system that has been infiltrated by terrorist.

It is crucial to reflect on the above scenarios. In order to throw more light on, and open the floor for more discussions, Let's look at, in more technical terms, some critical infrastructure such as electricity supply system, Oil and gas industry, Pharmaceutical industry, Aviation Industry, Domestic Water supply system, implications when compromised, possible ways they are compromised, the need to give detail and invested attention to securing these infrastructures using cryptosystems.

In this write up we shall look at the use of cryptography within critical infrastructure capabilities, the awareness, the threats and the future.

Keywords

SCADA, ICS, Cryptography, Voltage transformer, sensors, Digital Air Traffic Control, DES, RSA, Certificate Authority, Cloud cryptography, Public key Infrastructure PKI, Cipher, HSM, Secure Hash Algorithm(SHA) Encryption, Decryption, symmetric key, Asymmetric key, Quantum cryptography.

1 Introduction

Increasingly, critical infrastructure relies on internetconnected industrial control systems and internet-enabled distributed operations. Industrial Control Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA), which control and automate core industrial processes, are central to the operation of infrastructure in electricity, transportation, oil and gas, water, manufacturing, and other critical infrastructure sectors. These systems and other technologies communicate constantly with sensors, actuators, meters, and enterprise devices through communications channels that, if compromised, can lead to catastrophic disruptions to essential services and loss of assets. Let's look at some of these critical infrastructures, underlying security risk factors and threat to property and life, and secure technology communication in this critical infrastructure.

Electricity supply infrastructure

Comprise of network of cables carrying high voltage power, bulk supply stations, sensors, meters, transformers to mention few. Distribution and monitoring also made possible through communication between network devices and industrial control systems. The connected devices can be a conduit for the threat actor to infiltrate the infrastructure to wreck a suicidal havoc. The wide coverage of distribution system and the enormous impact it can carry when a system go wrong, has national security implication. In December 2015, more than 230,000 Ukrainians in three different regions suddenly found themselves without electricity on a cold winter evening. A single, coordinated attack had taken down 30 public power substations. Hence the need to secure the infrastructure from compromise.

Water treatment plants

To make water fit for domestic use, treatment of the water is regulated by the right proportion use of chemicals, and deliver it at the right temperature and pressure on February 5, 2021, a hacker initiated an attack on Florida water treatment facility which briefly adjusted the levels of sodium hydroxide from 100 parts per million to 11,100 parts per million.

Energy infrastructure is critical to modern economies. According to Deloitte, the average large-scale oil and gas company uses half a million processors just for oil and gas reservoir simulation; generate, transmits and store petabytes of sensitive and competitive field data. An oil refinery temperature regulation system can be compromised and manipulated to cause suicidal attack, when access is gained into the infrastructure's control system.

Aviation industry

Play national and international roles of transport system with a very critical network on which its operations dwell. if this network is not well secured. Malicious actor can possibly gain and destroy both the reputation of the industry and national assets. The major systems frequently exposed to cyber threats in the aviation industry are aircraft IP networks of flight, Digital Air Traffic Control In August 2022, cyber-attack was launched against Portuguese airline, DDoS targeted key Taiwanese website just before House of Representatives Speaker Nancy Pelosi arrived in Taiwan.

2 Use Case: Encrypting your ICS communication

Based on my real work experience, I am telling a story where most of the cryptography and critical Infrastucture items will be explained, within a scenario and kind of environment, the facing problems/issues, possible solutions and takeaways.

Encryption is critical to the security of industrial control systems and the communications channels through which they send and receive sensitive data to keep critical infrastructure functioning. For example, encryption is used to protect data in transit across the electricity grid, including communications to and from operations centers, power generation systems, distribution stations, and home. Taking a brief look at some encryption standards, institutions will have to adopt the best practices and standards that best secure their critical infrastructure.

The primary objective of using cryptography is to provide confidentiality, data integrity, authentication and non-repudiation. Aside observing all security protocols, critical infrastructure must incorporate all the cryptography primitives, namely encryption, hash function, message authentication code (MAC) and digital signatures to secure their interconnected devices and control systems of their operational technology.

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. Divided into two, we have

1. **Symmetric Key Encryption**: The encryption process where same keys are used for encrypting and decrypting information for example: Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

2. **Asymmetric Key Encryption**: The encryption process where different keys are used for encrypting and decrypting the information. Ie using mathematically related public key and private key to encrypt and decrypt plaintext and ciphertext respectively.

Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication. With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be non-practical due to

challenges it faced for key management. This gave rise to the public key cryptosystems.

The most important properties of public key encryption scheme are:

• Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.

• Each receiver possesses a unique decryption key, generally referred to as his private key.

• Receiver needs to publish an encryption key, referred to as his public key.

Data Integrity

In the use of symmetric and public key schemes to achieve the confidentiality of information, data integrity is another cryptographic techniques designed to provide other security services. Threats to Data Integrity: When sensitive information is exchanged, the receiver must have the assurance that the message has come intact from the intended sender and is not modified unintentionally or otherwise. There are two different types of data integrity threats, passive and active.

Hash Functions

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. They are extremely useful and appear in almost all information security application. Values returned by a hash function are called message digest or simply hash values. Some popular Hash functions:

• Message Digest (MD). comprising a family of MD2,MD4, MD5,AND MD6

• Secure Hash Function (SHA). SHA-0, SHA-1, SHA-2 FAMILY

• The RIPEMD (RIPE Message Digest) is an acronym for RACE Integrity Primitives Evaluation Message Digest. This set of hash functions was designed by open research community and generally known as a family of European hash functions.

• Whirlpool. This is a 512-bit hash function.

Applications of Hash Functions

There are two direct applications of hash function based on its cryptographic properties.

• Password Storage: Hash functions provide protection to password storage.

• Data Integrity Check: Data integrity check is a most common application of the hash functions

MESSAGE AUTHENTICATION

Message authentication can be provided using the cryptographic techniques that use secret keys as done in case of encryption. Message Authentication Code (MAC): MAC algorithm is a symmetric key cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key. Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.

DIGITAL SIGNATURE

Digital signatures are the public-key primitives of message authentication. physically, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message. Similarly, a digital signature is a technique that binds a person/entity to the digital data. The binding can be independently verified by receiver as well as any third part. Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer. In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message.

There are three types of **Public Key Encryption** schemes:

1. **RSA Cryptosystem**

This cryptosystem is one the initial system. It remains most employed cryptosystem even today. The system was invented by three scholars Ron Rivest, Adi Shamir, and Len Adleman and hence, it is termed as RSA cryptosystem.

2. **ElGamal Cryptosystem**

ElGamal cryptosystem, called Elliptic Curve Variant, is based on the Discrete Logarithm Problem. It derives the strength from the assumption that the discrete logarithms cannot be found in practical time frame for a given number, while the inverse operation of the power can be computed efficiently.

3. **Elliptic Curve Cryptography (ECC)**

The cryptographic tools and protocols its security is based on special versions of the discrete logarithm problem. It does not use numbers modulo p. ECC is based on sets of numbers that are associated with mathematical objects called elliptic curves. There are rules for adding and computing multiples of these numbers, just as there are for numbers modulo p.

It is believed that the discrete logarithm problem is much harder when applied to points on an elliptic curve. This prompts switching from numbers modulo p to points on an elliptic curve. Also an equivalent security level can be obtained with shorter keys if we use elliptic curve-based variants.

3 Public Key Infrastructure

The most distinct feature of Public Key Infrastructure (PKI) is that it uses a pair of keys to achieve the underlying security service. The key pair comprises of private key and public key.

Key Management

Any cryptosystem depends upon how securely its keys are managed. Without secure procedures for the handling of cryptographic keys, the benefits of the use of strong cryptographic schemes are potentially lost. Public Key Infrastructure(PKI) provides assurance of public key. It provides the identification of public keys and their distribution. PKI comprises of the following components:

• Public Key Certificate, commonly referred to as 'digital certificate'.

• Private Key tokens.

• Certification Authority.

• Registration Authority.

• Certificate Management System.

Digital Certificate

People use ID cards such as a driver's license, passport to prove their identity. A digital certificate does the same basic thing in the electronic world, but with one difference. Digital Certificates are not only issued to people but they can be issued to computers, software packages or anything else that need to prove the identity in the electronic world.

• Digital certificates are based on the ITU standard X.509 which defines a standard certificate format for public key certificates and certification validation. Hence digital certificates are sometimes also referred to as X.509 certificates.

• CA digitally signs this entire information and includes digital signature in the certificate.

• Anyone who needs the assurance about the public key and associated information of client, he carries out the signature validation process using CA's public key.

Certifying Authority (CA)

CA issues certificate to a client and assist other users

to verify the certificate.

The key functions of a CA are as follows:

• Generating key pairs – The CA may generate a key pair independently or jointly with the client.

• Issuing digital certificates – The CA could be thought of as the PKI equivalent of a passport agency - the CA issues a certificate after client provides the credentials to confirm his identity. The CA then signs the certificate to prevent modification of the details contained in the certificate.

• Publishing Certificates – The CA need to publish certificates so that users can find them. There are two ways of achieving this. One is to publish certificates in the equivalent of an electronic telephone directory.

• Verifying Certificates – The CA makes its public key available in environment to assist verification of his signature on clients' digital certificate.

• Revocation of Certificates – At times, CA revokes the certificate issued due to some reason such as compromise of private key by user or loss of trust in the client. After revocation, CA maintains the list of all revoked certificate that is available to the environment.

• There are four typical classes of certificate:

o Class 1: These certificates can be easily acquired by supplying an email address.

o Class 2: These certificates require additional personal information to be supplied.

o Class 3: These certificates can only be purchased after checks have been made about the requestor's identity.

o Class 4: They may be used by governments and financial organizations needing very high levels of trust.

Registration Authority (RA)

CA may use a third-party Registration Authority (RA) to perform the necessary checks on the person or company requesting the certificate to confirm their identity.

Certificate Management System (CMS)

It is the management system through which certificates are published, temporarily or permanently suspended, renewed, or revoked.

Private Key Tokens

While the public key of a client is stored on the certificate, the associated secret private key can be stored on the key owner's computer. This method is generally not adopted. If an attacker gains access to the computer, he can easily gain access to private key. For this reason, a private key is stored on secure removable storage token and/or on Hardware Security Modules (HSM) access to which is protected through a password.

Post-Quantum Cryptography

Post-quantum refers to cryptographic methods that are secure against attacks from quantum computers. Quantum computing offers great potential to solve critical problems – but it also presents challenges that will require new technologies and partnerships to tackle.

Speaker and References

Soenil Soebedar is a solution-oriented IT cyber security professional who spent more than 30 years in the IT sector, 20 years as a contractor and founder of SOEBIT Cybersecurity in Netherlands (Europe) and 10 years in the Cyber Security field as Ethical Hacker, Penetration tester, PKI/Cryptography specialist & Architect, Senior Security Engineer, Senior SOC Specialist. Speaks 4 languages : English, Dutch, Hindi & Bhojpuri (East-India).

He has experience in a number of industries such as

Finance and Banking, Energy, (Dutch) Government, Healthcare, Education and Consulting and a lot of international experience to work in teams and individually, in multiple countries and several cultures: France, Germany, UK, The Netherlands, Belgium, India, USA, Suriname, Singapore & Dubai.

Technical & Keynote Speaker:

• 2023: ICICACS – IEEE Conference (Online) - India – Keynote speaker

• 2022: C0c0N XV – Police Hacking & Cybersecurity Conference Kochi - India – Technical speaker

• 2022: MYSURUCON – IEEE Bangalore India Conference (Online) Keynote speaker

• 2021 & 2022: Rocheston REINVENT USA – Cybersecurity Conference (Online) Technical speaker

• 2021: MYSURUCON – IEEE Bangalore India Conference (Online) Technical speaker

• 2021: DIVERSECCON – DEVSECOPS Conference (Online) Technical speaker

• 2021: Next Generation CyberMinds, Malaysia Conference (Online) Technical speaker & Workshop

• 2019 till now: Speaker on monthly bases on Webinars & Workshops for Colleges & Universities in India in Hindi & English.

• 2016 till now: Speaker on virtual workshops, cybersecurity training, Webinar & Conferences for Students, IT Professionals, in The Netherlands, USA, Suriname, India, Ghana, Singapore & Malaysia.

Summary Work Experience only Cybersecurity assignments:

• 2022 till now: Working (part-time) as freelance Senior PKI Cryptography specialist for Dutch Central Bank in Netherlands.

• 2022 till now: Working as freelance Cryptography Architect for Government of Defence in The Netherlands.

• 2021 - 2022: Worked 16 months as freelance Senior Cloud Security Engineer for ABN-AMRO Bank in Netherlands.

• 2019 - 2021: Worked 3 + Years for the Government of The Netherlands – Division: Ministry of Justice and Security for customers as Custodial Institutions Agency (All Prisoner of NL) as Senior SOC Security Engineer & Medior Penetration Tester.

• 2016 – 2020: Worked 5+ years in the IT & Cybersecurity Training & Education field – International (Netherlands, Dubai & India)

• 2011 – 2017: Worked 7 + years for the European Power & Gas exchange market in France as Senior PKI Engineer.

Summary Training & Certifications:

• Hold 24 International cybersecurity certifications Of Microsoft, Rocheston & EC-Council: such as (CEH) Ethical Hacker, RCCE (Cybersecurity Engineer), RCCS, CCISO, Computer & Mobile Forensics CHFI, Cryptography Specialist (ECES), Incident Handler, Disaster Recovery & advanced penetration testing, Microsoft Azure SC-900, SC-200, AI-102, etc.

• Certified Trainer for EC-Council & Rocheston (technical) cybersecurity training.

White Paper

Generative AI-Powered Live, Virtual, and Constructive Training Events

NATO CA2X2 FORUM 2023

Pytho AI

Contact: mike@pytho.ai

Executive Summary

Pytho AI's goal is to provide NATO and the Intelligence Community (IC) with the ability to design and execute the most impactful live, virtual and constructive (LVC) training events to maintain readiness and prepare warfighters for the challenges of modern conflict. Our generative AI platform is the perfect human-machine teaming solution that significantly improves warfighter readiness through:

- *Generating Realistic and Dynamic Scenarios: No more stale or reused scenarios. Pytho generates novel and realistic scenarios that reflect the complexities of modern warfare.*
- *Making Better Decisions: Data is synthesized and summarized immediately. Commanders will get key information quickly to reduce the fog of war.*
- *AI Education and Training: Warfighters engage with and learn the principles of artificial intelligence with an AI copilot in a training environment.*
- *Saving Time, Capital, and Resources: Reduce the time, effort, and resources needed to design and execute training events.*

Section 1: Introduction

"The general who wins the battle makes many calculations in his temple before the battle is fought. The general who loses makes but few calculations beforehand."

- Sun Tzu, The Art of War

1.1 Problem Statement

Planning and executing wargames and NATO training exercises is:

- Time consuming
- Resource intensive
- Expensive
- And the planning process does not always lead to challenging, immersive, and engaging training

Military training is the foundation of combat readiness; it builds the skills and the confidence needed to succeed in the most challenging and demanding environments. NATO leaders have been clear that they view the digital battlefield as the battlefield of the future. And if software is the key to success in future conflict, the military's wargames and training exercises must adjust to reflect this reality. How can NATO and the IC plan and execute training events faster, more efficiently, across all domains,and with greater realism, to ensure that our military and intelligence community is fully prepared for any challenges they may face?

1.2 Solution Abstract

Recent advances in generative AI, specifically large language models and diffusion, allow warfighters to design and execute more realistic training scenarios that closely simulate the real-world environment. Pytho's generative AI platform streamlines and enhances LVC planning and maximizes the impact of the training for warfighters in minutes compared to months.

1.3 Operational Impact

The largest military training exercises take 18+ months to plan. Even the smallest exercises and wargames conducted at military school houses or on tabletops require significant planning and remove

warfighters from their normal operational demands. What if planners had a copilot to assist with scenario design and execution, allowing for faster iteration, more creativity, and increased scalability of training events?

Participating in live, virtual, and constructive training can be boring and feel more like a command requirement than actually enhancing readiness. What if participants were exposed to new, highly realistic and dynamic training scenarios that challenge their decision-making, problem-solving, and communication skills, all while learning about artificial intelligence?

The progress made in generative AI now makes this a reality, and models can now serve as "copilots" to support wargames and training exercises in ways that were not possible before. Pytho's applications to warfighters and the intelligence community include but are not limited to:

Planners

- Design realistic scenarios and vignettes
- Write dynamic scripts
- Define training objectives and metrics
- Model and generate realistic opponents
- Create role playing guidelines
- Rapid prototyping to quickly test game mechanics and scenarios
- Develop multi-modal orders, plans, and instructions
- Generate injects at scale to simulate the information environment

Participating Warfighters

- Summarize neverending data and rapidly find trends or detect anomalies
- Develop and recommend courses of action
- Draft functional intelligence reports and operational products
- Automate real-time alerts
- Search and retrieve relevant information
- Real-time analysis of gameplay or exercise performance

After Action Review

- Log and summarize key points
- Inform future exercises and training events
- Recommend lessons learned and opportunities to leverage

Section 2: Technical Approach

2.1 Technical Approach

Pytho leverages cutting-edge artificial intelligence technology to allow warfighters to harness the power of large language models to reduce their cognitive burden and enhance their training and readiness:

Large Language Models: Natural language processing (NLP) has advanced significantly over the last few years with the introduction and improvement of transformer models. Unlike previous NLP models, which relied on predefined rules and patterns to process text, transformer models use a neural network architecture that can dynamically learn and generate language representations from vast amounts of data. We use state of the art transformer models to generate high-quality, diverse, and dynamic scenarios that are tailored to the specific needs and objectives of military training exercises. These transformer models revolutionized the implementation of attention, allowing them to dynamically and selectively focus on different parts of the input text, enabling them to generate more

accurate, diverse, and contextually relevant responses to prompts.

Fine-Tuning: The ability to generate realistic and adaptive responses is crucial for developing service members' readiness and effectiveness in high-stress situations. To ensure that our models are continuously improving and evolving, we rely on a variety of techniques and data sources:

- *Training data with context*: We fine-tune our models on data relevant to military training and wargaming, so that our transformer models are especially well-suited for military training scenarios; this ensures that our models are continuously updated with the latest terminology, phrasing, and context-specific information that warfighters are likely to encounter.

- *Reinforcement Learning from Human Feedback (RLHF)*: By using RLHF, our transformer-based models learn to better understand and respond to human preferences and expectations and optimize performance for the warfighter task at hand.

- *Prompt-tuning*: We also utilize prompt tuning to further optimize our models. Prompt tuning involves refining our models' responses to specific prompts by analyzing and adjusting the parameters to ensure the model provides the most relevant and accurate responses to each unique prompt.

Explainability: The increasing integration of AI in military operations has highlighted the paramount importance of explainability, as it enables trust, safety, compliance, transparency, audibility, adaptability and human-in-the-loop decision making, making it a crucial aspect for the successful deployment of military AI models. Our technology is not going to replace human operators; it will strengthen human-machine teaming to produce powerful and trustworthy results that show why results are shown and recommendations are made.

Security: Amazon, JPMorgan Chase, Verizon, and other companies are not allowing their employees to use ChatGPT due to concerns about data security. Even Italy restricted the use of OpenAI's technology over privacy concerns. Samsung employees accidentally shared confidential information, including confidential source code and internal presentations, while using ChatGPT for help at work. With Pytho, NATO forces do not have to worry about warfighters sharing sensitive data because users get individual inference instances, deployed on-prem or in a virtual private cloud, so the platform is optimized for security.

Infrastructure Agnostic: Our technology is infrastructure agnostic, leveraging a containerized platform. It is easily integrated with existing infrastructure, enabling warfighters to benefit from the advantages of large language models without having to make any changes to their existing infrastructure. This makes it easy for military planners and participants to adopt our technology and start generating more realistic and effective training scenarios right away, without having to invest in new hardware or software. Moreover, our technology is designed to be flexible and scalable, allowing us to adapt to the specific needs and requirements of different military branches, units, and missions. Whether it is simulating a high-intensity combat scenario or a peacekeeping operation, our infrastructure-agnostic approach ensures that service members receive the most realistic and effective training possible.

Section 3: Team Qualifications

3.1 Team

We are a team of builders with a history of shipping production ready machine learning software. Mike and Shah have a combined 25+ years of experience leading technology teams. The team operates with a bias toward action and prioritizes getting feedback from the warfighters on the ground to optimize the product.

Mike Mearn (CEO)

- *Background*: Mike is a former United States Marine Corps Officer and he led human intelligence teams

for the Marine Corps in the most kinetic region of Afghanistan. He deeply understands the need to win the decision advantage and to get information as fast as possible to the people that need it most. During his service in Afghanistan, Mike's teams were responsible for disrupting Taliban operations and protecting coalition forces. He also has extensive product management experience and has led technical and non-technical cross-functional teams in San Francisco at Facebook and unicorn startups.

● *Education*: BS, United States Naval Academy. MBA, Harvard Business School.

Shah Hossain (CTO)

● *Background*: Shah has over ten years of experience in cloud, data, and machine learning. He began his engineering career at Amazon and then set out on the path to lead machine learning teams, challenging himself as a founding engineer at startups and spending the last four years leading machine learning teams at Fanatics.

● *Education*: BS in Computer Science, Bangladesh University of Engineering and Technology. MS in Computer Science, Wayne State University. AI Professional Program, Stanford University.

Section 4: Funding

Pytho is venture capital backed and will continue to raise funding from the venture capital community in order to bring innovative products to market to support warfighters and the intelligence community.

Section 5: The Future

Deploying large language models is just the beginning. NATO operates in a multi-modal data environment, one which we will support with multi-modal data fusion.

Legal Roles in Exercises and Wargames

Sara Mubarek AlHajri,
sara_mubarak_alhajri@outlook.com
Najlaa Haza AlHajri, najlaa.hz@hotmail.com
Joint Warfare Training Center - Doha, Qatar

Erdal Çayırcı, erdal@dataunitor.com
Dataunitor AS - Stavanger, Norway

Abstract

Legal advisors are among the key contributors in wargames and exercises. Their support is broadly categorized as legal advice and legal play. Legal advice can be related to real life issues or about scenarios including main incident list, such as, the compliance with national and international laws. Controllers and players especially in operational and higher level command post wargames and exercises may very often seek for legal advice on their decisions. During the conducting stage, legal players have the following major roles: observer/trainer, protagonist and role player. In foundation training before the execution, a good coverage of the national and international law is typically necessary. In execution, various legal injects can be made as a part of main incident list, which requires role play. Apart from this, legal advisors can always bring up the legal issues and implications related to every action taken by the players/training audience even when the action is not directly related to a legal play. In this presentation, we first explain the significance of legal content. We elaborate on the international law and the law of war. Then, we focus on the tasks related to legal advice. Later we give the details about the dynamics of legal play during the conducting stage. Finally, we conclude our presentation.

1 Introduction

International law is made up of norms and principles that apply to all situations and deal with how states and international organizations should behave in their interactions with other nations, as well as with private citizens, minority groups, and multinational corporations. International law has several sources, including treaties, customs, and general law principles. Treaties are contracts between two or more states that produce legal obligations between them. Customary international law, on the other hand, is a collection of unwritten rules and practices that governments generally accept. General principles of law are accepted legal standards by all national judicial systems in the globe. The basis of international law is a number of fundamental ideas, such as equality, sovereignty, and the peaceful resolution of disputes. The notion of a state's right to rule its territory independently is known as sovereignty. Equality indicates that all states, regardless of size, population, or economic strength, are equal under international law. The peaceful resolution of disputes implies that states should settle their issues through peaceful means such as mediation or negotiation rather than resorting to force.

Human rights are also one of the most prominent topics of international law. International human rights law is based on the idea that everyone, regardless of nationality or other characteristics, is entitled to certain fundamental rights and liberties. These rights include the right to live, security of persons, liberty, and freedom from discrimination, torture, and arbitrary detention.

To summarize, international law is necessary for facilitating cooperation, peace, and respect for human rights in the global community. It depends on a collection of principles and sources that are continuously growing to fulfill the world's changing needs. In addition, by promoting the amicable settlement of conflicts and upholding basic human rights, international law plays an important role in building a more equitable and stable world.

Law of War has both international and national components and must be incorporated into military education and training activities including wargames and exercises. Legal roles in wargames and exercises

are depicted in Figure 1. In this paper, we elaborate on these roles.

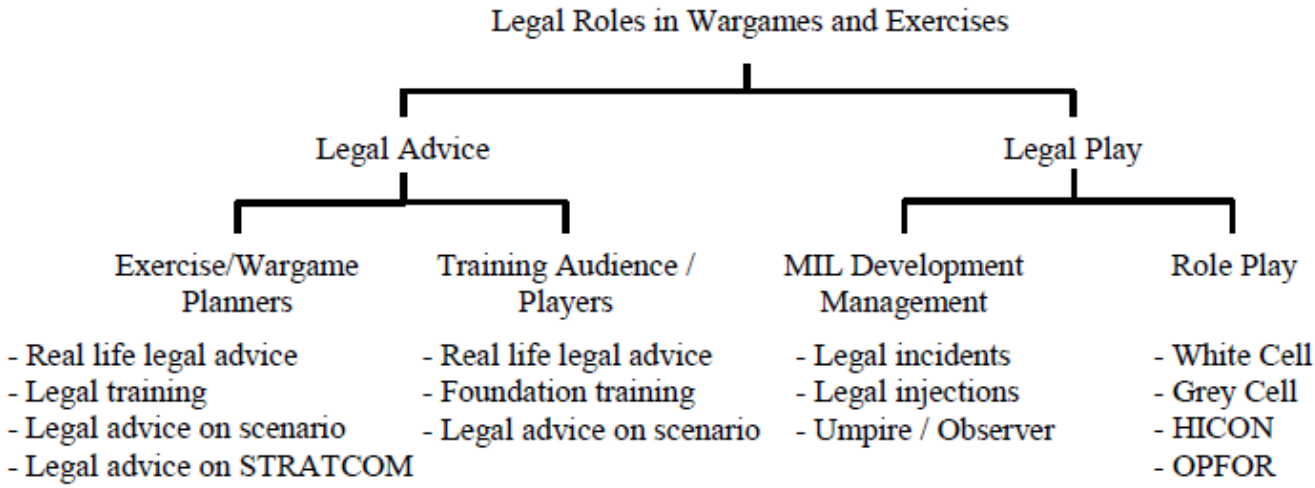


Figure 1. Legal roles in wargames and exercises.

In Section 2, we first briefly introduce law of war. As illustrated in Figure 1, legal roles in an exercise/wargame can be grouped into two as legal advice and legal play. Section 3 is dedicated to legal advice and Section 4 is on legal play. The paper is concluded in Section 5.

2 The Law of War

The law of war is that part of international law dealing with the inception, conduct, and termination of warfare. Its goal is to reduce the suffering caused by combatants and, more specifically, those who can be classified as war victims, namely noncombatant civilians and those who are no longer able to participate in hostilities. As a result, the injured, sick, shipwrecked, and prisoners of war deserve legal protection as well. Law of war has the same substantive meaning of international humanitarian law. In other cases, international humanitarian law is understood more narrowly than the law of war. The rules of war, sometimes known technically as international humanitarian law, are a set of international norms that govern what can and cannot be done during an armed conflict. The main purpose of international humanitarian law (IHL) is to maintain some humanity in armed conflicts by saving lives and reducing suffering. To that end, IHL governs how battles are waged, balancing two factors: weakening the opponent and minimizing suffering. The rules of war apply to everyone. The Geneva Conventions, which are the core elements of IHL, have been ratified by 196 states. This kind of support is found in very few international treaties. Everyone fighting a war, both government forces and non-state armed groups, must adhere to IHL. There are repercussions for breaking the rules of battle. States and international courts document and investigate war crimes. Individuals can be charged with war crimes.

The First Geneva Convention of 1949, referred to in shorthand as GC I, protects wounded and sick members of armed forces in the field. It provides rules for the protection of medical personnel, the evacuation and treatment of the wounded and sick, and regulates the use of protective emblems such as the Red Cross and Red Crescent. The Second Geneva Convention, or GC II, similarly protects the wounded, sick, and shipwrecked members of armed forces at sea. The Third Geneva Convention, or GC III, provides protection to prisoners of war. It provides rules regarding their capture, their internment, and their release and repatriation. The Fourth Geneva Convention, or GC IV, provides protection for civilians in times of armed conflict and

lays down rules relating to the occupation of territory by hostile forces.

The First Additional Protocol of 1977, or AP I, provides additional rules relating to international armed conflicts, including rules on the conduct of hostilities and the protection of the civilian population. The Second Additional Protocol of 1977, or AP II, provides a far smaller body of rules relating to certain types of non-international armed conflicts, including treatment of the wounded and sick and protection of the civilian population. The Third Additional Protocol of 2005, or AP III, provides for the use of an additional protective emblem.

Since every state in the world has ratified the four 1949 Conventions, they therefore necessarily apply to every armed conflict the world over. Additional Protocols I and II have been ratified by 174 and 168 states respectively, and therefore have wide, but not universal, application. They only apply as a matter of treaty law in conflicts between or within ratifying states (Tippett,2018).

3 Legal Advisor Support to Wargames and Exercises

Legal advisor support is needed for three purposes during an exercise process: legal advise to real life issues, legal advise to exercise content, such as scenario and main incident list and legal advise to course instructions during foundation training (Cayirci 2023). Legal advice can be related to real life issues, such as, about the legal implications of a memorandum of understanding and the compensation of various actions. Legal advice can also be about scenarios including main incident list, such as, the compliance with national and international laws. Controllers and players especially in operational and higher level command post wargames and exercises may very often seek for legal advice on their decisions.

The Legal Advisor (LEGAD) provides expert legal advice, technical guidance, and other assistance to the Command Group and the Staff to ensure the HQ complies with all governing treaties, international agreements, and applicable laws to ensure compliance with Qatar Armed Forces (QAF) policy and guidance and Ministry of Defense (MOD) obligations in the functional areas for legal support. Both civilian and military lawyers may act as legal advisers to the commander. The LEGAD will advise the commander in broad terms on the following: international law and legislation and mandates for the mission; the legal aspects of the use of force and the rules of engagement (ROE); legal aspects relating to allies, partners and the host nation; all legal matters ensuing from the physical presence of the joint force on foreign territory (status of forces agreements, memoranda of understanding, technical agreements). The legal support concentrates in two major areas:

- Area 1 Operational Law: This includes international regulations and policies that directly affect military operations across the spectrum, from peacetime activities to combat operations, and providing training to assigned staffs, forces, subordinate units, or individual service members and civilian personnel. It also includes participation in the experimental testing of new concepts that are independent of education and training activities. Provide legal reach-back to Legal Advisors in-theatre operational headquarters on complex juridical issues raised through the chain of command.

- Area 2 Fiscal, Contracting and Administrative Law: This includes procurement advice and support, interpreting financial rules and procedures as may arise in headquarters' activities, stationing and garrison requirements, and operations. Advice related to the payment of damages for harm caused by QAF forces, including ex gratia payments Administrative law, including employment law, privileges and immunities, environmental law, applicable host nation or sending state laws and regulations, and standards of conduct. Pleading or preparing cases (affirmative and defensive court actions) before both international and host nation forums and courts, as well as at QAF administrative tribunals fall in this category. Legal advisors provide

further legal assistance to commands, activities, and multinational entities as directed by the commander, as well as, other support to ad hoc integrated project teams.

From a legal perspective, military exercises are typically conducted within the framework of domestic and international law. The specific laws governing military exercises may vary between countries, but there are accepted principles and guidelines that are followed. Here are some important factors to consider:

- National Laws: Each country has its own legal framework that governs military exercises conducted within its territory or by its armed forces. These laws may include regulations related to the use of military force, protecting human rights, environmental considerations, and the authority under which the exercises are conducted.

- International Law: Scenarios, MIL and all actions during a military exercise must comply with international law, including treaties, conventions, and customary international law. This is critical not only for the training purposes but also strategic communications both to the exercise audience and public. The more law compliance is underlined in exercise, the better it is internalized by the training audience. Some relevant areas of international law with this respect include:

a. Law of Armed Conflict (LOAC)/International Humanitarian Law (IHL): These laws regulate the conduct of hostilities and seek to protect civilians and combatants who are no longer taking part in the hostilities as explained in the previous section. The content and actions in military exercises must comply with these laws.

b. United Nations Charter: The UN Charter prohibits the use of force between states except in cases of self-defense or when allowed by the UN Security Council. Military exercises should not violate the principles outlined in the UN Charter.

c. Treaties and Agreements: Bilateral or multilateral agreements between countries can regulate military exercises. These agreements may cover issues such as notification procedures, limits on the scale or duration of exercises, and restrictions on the use of certain weapons or areas.

- Diplomatic Considerations: Before conducting military exercises abroad, countries usually engage in diplomatic channels to seek permission or inform the host nation. These diplomatic negotiations help ensure that the exercises are conducted within the legal framework of the host country.

- Safety and Environmental Regulations: Military exercises must also adhere to safety regulations to prevent accidents and protect the health and well-being of personnel involved. Environmental regulations may be in place to minimize the impact of exercises on natural resources, protected areas, and ecosystems.

It is important to note that each country's legal framework and interpretation of international law may differ, and what is legal in one jurisdiction may not be viewed the same way in another. There may be situations where legal frameworks are not followed or disputed, leading to legal controversies or international tensions.

4 Legal Play During the Conducting of Wargames and Exercises

During the conducting stage, legal players have the following major roles, observer/trainer, protagonist and role play. In foundation training before the execution, a good coverage of the national and international law is typically necessary. In execution, various legal injects can be made as a part of main incident list, which requires role play. Apart from this, legal advisors can always bring up the legal issues and implications related to every action taken by the players/training audience even when the action is not directly related to a legal play.

Legality (the role of law), must be taken into account when planning, facilitating and conducting

wargames/exercises, in order to create an environment that will help the training audience to implement, test their decisions, and at the end meet their training objectives. Therefore, legal advisors should be involved in, not only all the execution stage, but also in the preparation of wargames/exercises:

- Trainer during foundation training: In the earlier stages of conducting a wargame/exercise, legal advisors play a major role in preparing and helping the players/training audiences to acquire the fundamental knowledge and learn the best practices in order to avoid any lack of information that could cause mistakes during the execution. Building the players knowledge can be delivered through various ways, for example: lectures presented by legal advisors, as well as group workshops where participants exchange their experiences. Since wargames/exercises are executed to simulate an operation, where players are required to make decisions and act as if it is a real life situation, it means that they are also required to abide by and apply pre-existing international treaties and laws, therefore, the training audience must have foundation training/lectures by legal advisors on topics, such as national law, the international humanitarian law and the law of armed conflicts. The legal advisor coverage of these topics help the training audience to ensure that their decisions and plans comply with the international regulations, and they are ethically wise.

- Observer/Trainer during execution: Moving along, during the wargame/exercise, the legal advisor plays a critical role in facilitating and making sure that players are on the right track, especially when a confusion accrues among the players. Furthermore, during execution, an instructor can explain an event in the game by providing real-world references.

- Role play during execution: The instructor/LEGAD should have the authority over the gaming process, where he or she is given opportunities to steer the learning process and challenge the players (Frank, 2014), and this requires a role play, where a LEGAD plays different roles in order to test the players on their knowledge in a number of subjects, for example, and not limited to, the extent of their knowledge and application of the rules of engagement of the game. Moreover, various injects can be made by the LEGAD during execution, not necessarily within a legal incident. For instance, an incident that requires the players to deal and cooperate with civil institutions can give an opportunity to inject few challenges related to law and ethics (Frank, 2014), (Taylor et al, 2012).

- Legal advice to training audience: LEGAD can help in filling the gap and upholding the link between the game (including the player's decisions) and the real world. The LEGAD duties during execution, and in preparation stage as mentioned previously, is to make sure that the players are aware, and act, abided and according to the intentional law and treaties. Moreover, the LEGAD role during a wargame is based on their role in wars, under Article 82 of the First Additional Protocol to the 1949 Geneva Conventions, which covers 3 areas: Advising commanders upon the application of the Conventions and of the Protocol, advising commanders in time of armed conflict upon those Parts, III and IV of the Protocol, which deal with the conduct of military operations and advising commanders upon the instruction to be given in the armed forces on those instruments. (Draper,). Hence, LEGADs support commanders in planning for their military operation and in the targeting process, where their advisory role is "reviewing the targets as subject matter experts in IHL/LOAC, and ensure that targeting efforts are aligned with the legal framework and that IHL/LOAC principles are integrated along the whole process from target discovery through validation and engagement (NATO STANDARDIZATION OFFICE, 2021). LEGAD role can be performed with request for further information and assessment from different unites and sources, such as the intelligence.

5 Conclusions

Subject matter experts from legal field have key roles in planning, programming, developing and conducting

wargames and exercises at all levels, most notably operational and strategic level command post exercises. Their contribution can be broadly categorized into two groups, legal advice and legal play. Legal advise is needed both by the exercise planner/controllers and training audience and include legal advice on real life issues, legal advise for scenario and STRATCOM, foundation training on the law of war/conflict. Role play require designing and scripting legal injections and actions and role playing as a part of white cell, grey cell, HICON and also opposing forces.

Acknowledgements

This research is supported by the Qatar Armed Forces General Headquarters.

References

Australian Government Pub. Service, Vienna Convention on the law of treaties (Vienna, 23 May 1969). entry into force for Australia: 13 July 1974 (1974). Canberra.

Emily, C. (2015). Geneva conventions additional protocol I (1977). *Max Planck Encyclopedia of Public International Law*. https://doi.org/10.1093/law:epil/9780199231690/e1804

Cayirci E., R. AlNaimi, and S.S.H. AlNabet. "Computer Assisted Military Experimentations," In Proceedings of the 2022 Winter Simulation Conference, edited by B. Feng, G. Pedrielli, Y.Peng, S. Shashaani, E. Song, C.G. Corlu, L. H. Lee, E.P.Chew, T. Roeder, and P. Lendermann, Singapore, December 2022a.

Experimentation Training Evaluation (ETE) A.Ş., "Computer Assisted Wargames, Experiments, Exercises," Volume 3: Exercises, Izmir, 2023.

Beckman, R., & Butte, D. (n.d). Introduction to International Law.

DoD Law of War Manual.

Frank, A. (2014). *The Instructor Role during Educational Wargaming.*

Pilloud, C, Sandoz, Y, Swinarski, C, & Zimmermann, B, Commentary on the additional protocols of 8 june 1977 to the Geneva Conventions of 12 August 1949 (1987). Geneva; International Committee of the Red Cross

Rowe, Peter John. "law of war". *Encyclopedia Britannica*, 9 Aug. 2022, https://www.britannica.com/topic/law-of-war. Accessed 20 August 2023

Taylor, A.-S. A. (2012). he Coaching Cycle: A Coaching-by-Gaming Approach in Serious Games. *Simulation & Gaming: An Interdisciplinary Jorunal*, 43(5).

"Quantum" Evolution in Europe

The Future of Cybersecurity

Giovanni Gasbarrone
ANUTEI Vice President
National Association of Italian Army Technical Officers

Abstract

Next generation "QUANTUM" technologies represent a revolution in military operations that will change in the future the way of operations, from cybersecurity to communications in tactics, operational and warfare strategies in modelling & simulation. Quantum technologies are dual-use technologies, and therefore are of interest to the defence and cyber security industry and military.

A fundamental role in this new scenario is "hyper connectivity" in the military framework as a digitization of the battlefield where all military elements are connected. The Defense Science Board (DSB), an independent Department of Defense (DOD) board of scientific advisors, has concluded that three applications of quantum technology hold the most promise for DOD: quantum sensing, quantum computers, and quantum communications. Today, European critical infrastructures and public safety communications and cloud are vulnerable to cyber-attacks. Today advances in supercomputing and the advent of quantum computing may soon undermine modern encryption systems, threatening the security of transmitted data and secure access to remotely cloud infrastructure.

1 "Quantum" Evolution in the Future of Cybersecurity

Quantum computers perform mathematical tasks thanks to Qbit. Quantum Computing will support the development of innovative services, and one of the new areas of research is the synergy of quantum computer with artificial intelligence (AI). The AI domain is a reality and therefore many applications will be deployed with AI to support next-generation wireless communications.

In fact, one of the industries that profit most from artificial intelligence technologies is that of wireless communications, as AI is incorporated into both smartphones and cellular architecture to control services and network resources.

The 6G network will manage billions of devices, thanks to quantum computing and artificial intelligence platforms. Digital technologies are also becoming a fundamental and essential means of guaranteeing the sovereignty of countries. The development of 6G infrastructure and solutions based in Europe is one of the keys to ensuring European sovereignty in critical technologies and systems.

For this strategic and vital goal for the survival of the Industry, the EU has launched a first research program of 240 million euros for 6G, thus hoping to maintain technological sovereignty after 5G also in 6G.

Among the innovative hyper connectivity technologies, the Software Defined Radio and Cognitive Radio will be able to adapt to changes in the environment, interference and the availability of licensed and unlicensed frequencies.

Thus contributing to the management of traffic in communications between different systems, even in operational scenarios that provide more flexible spectrum management methodologies thanks to "cognitive radio" & "self-organizing functionalities".

Cognitive Radio is the intelligent technology that explores the spectrum by exploiting the holes of unlicensed or underused frequencies and their spatial availability. In the 6G communication network, devices such as smartphones are expected to interact with the base stations of the cellular network and receive indications on the portion of the spectrum in which they can find more favorable

conditions in terms of greater availability for frequencies and bit rates.

This increases the complexity and the need for high computational capacity that can be met by Quantum Computing and Artificial Intelligence technologies. One of the main problems of a Cognitive Radio (CR) and SDR architecture for 5G systems is the enormous energy needs to support the cognitive capabilities of mobile devices. Cognitive Radio has a high complexity related to chip implementations and artificial intelligence applications. In addition, there are further limitations related to the realization of CRs that require devices with high computational complexities in order to analyse and perceive the entire spectrum range with good sensitivity and quality.

However, this evolution of 5G with the integration of SDR / CR in its 6G radio architecture even if now it appears an uphill road will become unavoidable.

The new "Next generation" 6G communication systems are already born intelligent, and will provide operators with a platform that will allow them to make the best use of the scarce resource of the spectrum thanks to an ethergeneous network architecture that requires cognitive radio to be realized.

The next decade will see 6G connect billions of device entities, sensors and connected vehicles, in a scenario where robots and drones will generate Zettabytes of digital information. 6G will improve 5G applications with more stringent requirements, such as holographic telepresence and immersive communication, and meet even stricter parameters than 5G.

Starting from 2030, we could see the advent of the era in which the use of personal mobile robotics will interact with next-generation Artificial Intelligence platforms thanks to neuronal systems offered by the connectivity of the 6G network.

6G is the generation of mobile networks that will help us to face the socio-economic challenges in which the way of living and working will make a new paradigm shift compared to 5G.

6G will be an autonomous ecosystem based on artificial intelligence. 6G will offer complete wireless connectivity almost instantaneous and without restrictions thanks to the cognitive radio in which artificial intelligence falls both in the mobile device and in the management of radio interfaces.

A new landscape will also emerge for industries and companies always involved in digital transformation thanks to the convergence that 6G will enable in the fields of connectivity, robotics, cloud computing. This will radically reshape the way companies operate while also changing future social relationships. This exposes us to risks of lack of development of microchips with autonomous technology in Europe. The topic is described in the article https://www.agendadigitale.eu/industry4-0/microchip-5g-e-cloud-cosi-la-ue-accelera-sui-pilastridella-trasformazione-digitale/

2 Next generation Cybersecurity : the reason why for Quantum Communication

• The cost of network attacks is doubling every few years

• An increasing need is envisaged for the development of disruptive applications in the areas of cryptography, cyber-security

• Finance transactions, public Telco Infrastructure and Defense communications may be secured with “quantum technologies” : Quantum key distribution (QKD) Quantum machine learning based on artificial intelligence application ;

• The EU strategy : the EuroQCI infrastructure

• It will integrate quantum cryptography and innovative and secure quantum systems into already deployed telecommunications infrastructures, enhancing them with an upper layer of security based on quantum technologies. The telco infrastructure architecture are already based on a terrestrial

segment relying on fiber communication networks connecting strategic ICT nodes at national and European level. The space segment is based on commercial and defense satellites, and it will provide additional links for national and cross border quantum communication networks across the EU and worldwide.

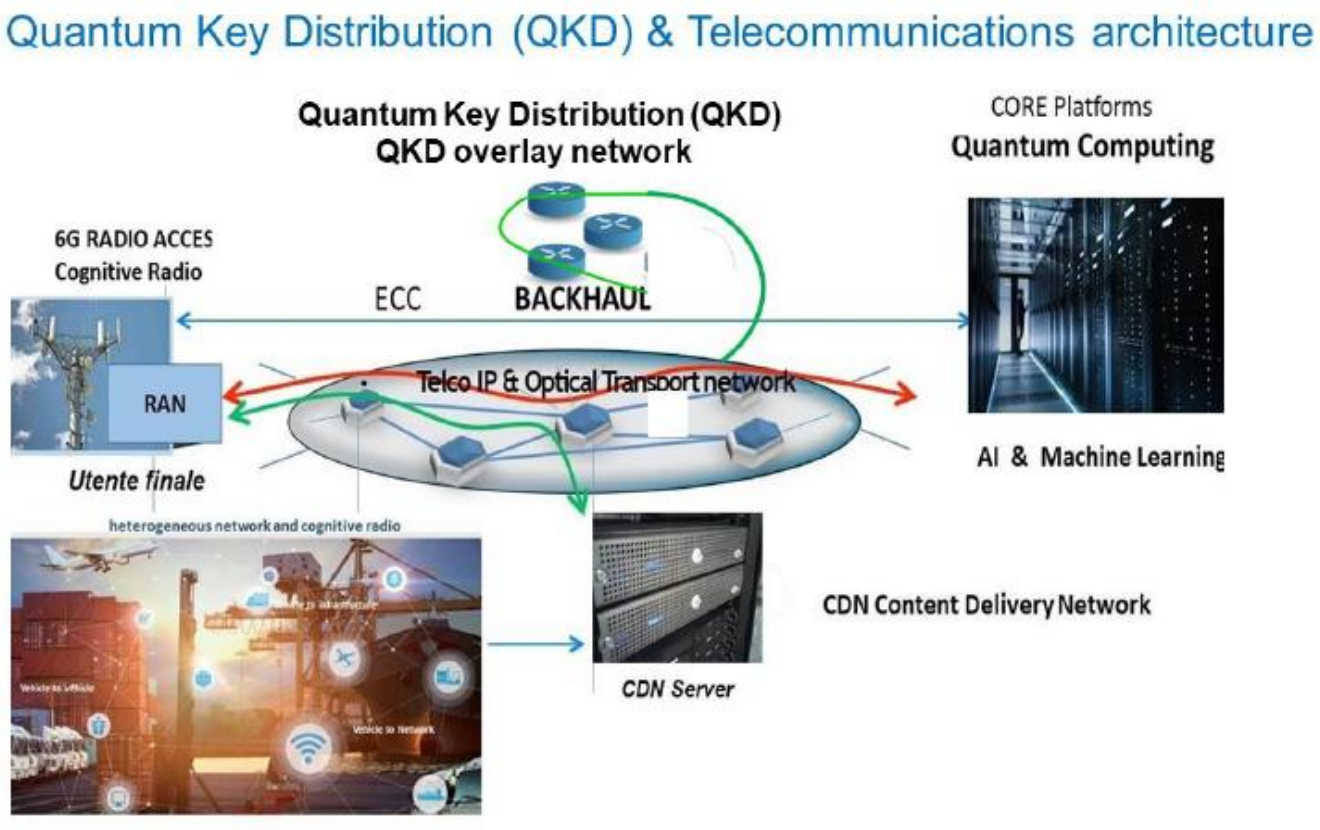
3 Quantum key distribution (QKD)

Unlike conventional encryption, quantum communication is considered unhackable and therefore the future of secure information transfer for banks, power grids and other sectors. The core of quantum communication is quantum key distribution (QKD), which uses the quantum states of particles—e.g. photons—to form a string of zeros and ones, while any eavesdropping between the sender and the receiver will change this string or key and be noticed immediatelyQuantum key distribution (QKD) is a secure communication method which implements a cryptographic protocol involving components of quantum mechanics.

It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages.

4 Quantum key distribution network deployment

Quantum key distribution will prevent cyber attack to sensitive data and critical infrastructures by integrating quantum-based systems into existing telecommunication and cloud infrastructures, providing an additional (over the top) security layer based on quantum physics.



5 EuroQCI quantum communication

The European Quantum Communication Infrastructure (EuroQCI) Initiative

There are 20 million euros available to develop, at national level, systems and networks that can test quantum communication technologies, with the aim of integrating them with existing communication networks and supporting the European Quantum Communication Infrastructure (EuroQCI).

https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

https://www.agendadigitale.eu/infrastrutture/5g-e-iot-per-gestire-le-reti-elettriche-limpatto-sullacybersicurezza-anche-delle-auto/

5G-proof cybersecurity, this is how "resilience by design" is available
https://www.agendadigitale.eu/infrastrutture/cybersecurity-a-prova-di-5g-cosi-nasce-la-resilience-by-design/

Cybersecurity for IoT and 5G, the strategic role of standards
https://www.agendadigitale.eu/sicurezza/cybersecurity-per-iot-e-5g-il-ruolo-strategico-degli-standard/

Security in the 5G revolution
http://channels.theinnovationgroup.it/cybersecurity/sicurezza-rivoluzione-5g/

Round table: cyber perimeter and data protection in the Internet of Things
http://www.anutei.it/index.php/associazione/regolamento/8-conferenze/28-tavola-rotonda- perimetro-cyber-data-protection-nell-internet-of-things

An Interoperable Generic Tool for Simulating Attacks within the Cyber Domain

Garratt Weblin, garratt.weblin@pitchtechnologies.com
Jonathan Denny, jon.denny@pitchtechnologies.com
Matt Tipper, matt.tipper@pitchtechnologies.com

Pitch Technologies UK,
5 Upper Montagu Street, London W1H 2AG

Abstract

In today's world, the constant threat of cyber-attack has grown substantially. Creating the need for realistic cyber training, enabling trainees to practice different scenarios in the safety of a simulated environment. This could range from modelling cyber behaviors and how they affect simulated assets, to Red vs Blue cyber duels where teams battle for control.

To aid development of interoperable cyber simulations, a SISO study group has developed a new standard, Cyber Data Exchange Model (DEM). An ontology that provides a common representation of cyber-attacks, events and objects to be used in simulation of the cyber domain.

As part of a Defence Science and Technology Laboratory (DSTL) research project, Pitch Technologies investigated the extent of the standards usefulness, given a specific use case based on real world scenarios. A high-level demonstration was created, using HLA, showing how the cyber domain could be simulated and integrated into existing simulations. This demonstration made use of multiple cyber-attacks to disrupt simulated government assets. A reusable generic cyber attacker was created, enabling cyber objects and interactions to be simulated inside an HLA federation. Future work with Cyber DEM could involve linking Red vs Blue and cyber influences software, enabling collective training. As well as integrating Cyber DEM into existing simulation solutions.

The Cyber DEM standard enabled the modelling of the given use case, to a high fidelity. Some interoperability challenges remained, as the standard is open to interpretation, it could be implemented in different ways, giving different results for the same events.

Cyber DEM and cyber attacker application only trigger cyber events, simulators must be able to react to these events. In most cases this would mean more development is needed to make use of the standard and tool. Due to the nature of open standards, plugins can be built for existing simulators expanding their scope and usefulness.

1 Introduction

1.1 The Cyber Domain

Unlike all other domains, the cyber domain is predominantly a virtual landscape, encompassing all digital communication and interactions. However, this does not mean it is any less important. It has become a key part of modern society and often dictates modern warfare. As technology evolves, so does the complexity of the cyber domain, making it harder to protect users from potential cyber-attacks whether that is social use by the general population, or different government agencies using the cyber domain for military and research purposes.

With 5.3 billion active users in 2022, the use of the internet is still growing all over the world. With an increase of over 4 billion users since 2005 [1], the internet has become the main resource for connecting people all over the world. Being more connected brings many benefits but also exposes users to new forms of attack. The most prominent form of cyber-attack that many face daily is phishing attacks through email and instant messaging platforms. These attacks aim to extract personal data and passwords from users, and then use this information to access more sensitive information like bank details. For businesses, this form of attack poses a significant threat and can lead to threat actors gaining access to sensitive systems with the potential for ransomware attacks. In 2022, in the UK, 18 ransomware attacks required nationally coordinated responses. With a further 63 incidents being nationally significant [2]. These numbers are on the

rise from previous years and are predicted to increase further in the future. For government assets and military especially, it is crucial that there are no sensitive data leaks or unauthorized access to secure systems.

1.2 Cyber Domain Simulation

Modeling & Simulation (M&S) can be used with great effect in several ways throughout the cyber domain including, networking simulation, software testing, cyber security training, and cyber warfare simulations. Simulated networks can be used to optimize network designs, improving performance and network resilience. Software pre-releases can be tested in contained environments to expose any common vulnerabilities and exposures (CVEs). Cyber security models can be used to train users on how to avoid and overcome common cyber-attacks. This involves simulating attacks, such as phishing attacks, to pinpoint key areas that require more formal cyber security training. Lastly, for military and defense purposes, cyber warfare can be simulated in safe managed environments. Allowing in-depth user training to develop offensive and defensive strategies.

1.3 Cyber Training

Throughout the cyber domain, there are already several training options available to become more cyber-aware. These range from awareness-level courses meant to make users aware of current threats and how to avoid them, to application-level courses, meant to give hands-on experience and a more in-depth look at how cyber-attacks come about and how to handle them. In the UK, the National Cyber Security Centre (NSCS) keeps track of available courses [3]. UK MOD is already strengthening the cyber skills of its personnel across all domains [4].

Several companies already subscribe their employees to online cyber security training, as part of the onboarding process but also through companywide simulated phishing attacks and cyber security refreshers throughout the year.

Red vs Blue training is a popular way to train cyber skills and test cyber defenses. Modeled after military training exercises, the Blue team acts as the "good guys", trying to prevent or respond to cyber-attacks on a given system. While the Red team acts as the "bad guys", trying to penetrate, infect, and extract data from the system. This method both tries to find vulnerabilities in a system and helps to train personnel on procedures should there be a breach.

When new cyber exploits are developed, the cyber security personnel are very much on the back foot. It is difficult to predict what will come next without prior knowledge. This brings the importance of staying up to date with previous and current cyber-attacks. The MITRE ATT&CK matrix is a knowledge base of various cyber phases for offense and defense [5].

1.3 Cyber Training Use Cases for Simulation

There are several use cases for training inside the cyber domain. Below are a examples of use cases tailored toward the defense industry.

Command and control (C2) System

Command and control (C2) systems are used to enable a centralized approach to facilitate decision-making, coordination, and communication. But what happens when the overview battle picture being used by the command is wrong? This could lead to incorrect commands being given, resulting in negative effects. For this use case, how can users be trained to identify when the current C2 picture may not be the actual ground truth and how do they act accordingly when the information they are receiving may not be correct? What measures can be taken to restrict access and increase security in the system?

Satellite Interference

An adversary could cause effects on the satellites that are supporting and providing information to platforms within the training environment.

These cyber-attacks affecting a satellite network could be particularly problematic for the training

audience as even minor errors could have significant implications, causing the systems to misrepresent the truth.

A jamming attack on the satellite's downlink can lead to a platform being unable to receive updates, such as positional information. Such an attack is likely to be quickly noticed by a trainee as it may have an effect similar to a malfunction. A training objective could be to understand how to mitigate this.

Another example would be if an attacker gains access to a satellite network and introduces an error in the timing source, causing the GPS receiver systems to misrepresent their spatial position. Methods for this include unauthorized access to a ground station able to control the network or an attacker introducing a device that can mimic the ground station.

Attacking in this way could be difficult for the training audience to notice, so a training objective might be to identify that this type of attack is occurring and what mitigating actions need to be taken.

2 Cyber DEM Standard

2.1 Overview

"The Simulation Interoperability Standards Organization (SISO) is an international organization dedicated to the promotion of modeling and simulation interoperability and reuse for the benefit of a broad range of M&S communities." [6]

Due to the rise of cyber interactions and the significant increase of research into cyber training throughout academia and industry, a SISO Product Development Group (PDG) was created and tasked with identifying key cyber activities, and lessons learned, and evaluating potential standardization areas within cyber modeling and simulation.

As part of this work, the Cyber Data Exchange Model (DEM) standard [7] is being developed, aiming to give a standard for representing cyber events and objects in a distributed simulation environment.

In practice, Cyber DEM is an architecture-agnostic ontology to enable bi-directional data exchange between cyber simulations. An ontology is a structured representation of knowledge that defines the concepts, their attributes, and the relationships between them within a specific domain, facilitating data integration and advanced reasoning in various applications. In this context, it allows for distributed simulations to test and train cyber interactions in the same environment.

The Cyber DEM Product Development Group (PDG) has created several mappings to common communication technologies, including support for and input to the following:

- High Level Architecture (HLA) Federation Object Model (FOM) (IEEE 1516)
- Input to the existing Distributed Interactive Simulation (DIS) standard (IEEE 1278)
- Input to the existing SISO enumerations (SISO-REF-010)
- Test & Training Enabling Architecture (TENA) Object Model
- JavaScript Object Notation (JSON)

2.2 Cyber DEM

The Cyber DEM standard is split into two main sections, Objects and Events. Objects are persistent in a simulation, for example, a physical device connecting to a network. Events are one-time messages that can happen during a simulation, for example, a phishing attack on a network.

2.2.1 Cyber DEM Objects

The Cyber DEM objects follow a hierarchy structure, with CyberObject being the base object. Therefore all other objects inherit from CyberObject, inheriting all its attributes. These objects can be used to represent a real-world network setup within a simulation.

Some more examples of objects available in Cyber DEM are:

- Network - A data network including LANs, WANs, tactical radio data networks, cellular data networks, etc.
- Device - An electronic device capable of operating in cyberspace.
- Persona - A user or profile for a person within cyberspace
- Data - Information encapsulated in an instance or collection of file(s), message(s), or record(s) in a database

The full list is available within the Cyber DEM standard.

2.2.1 Cyber DEM Events

As with objects, the Cyber DEM events follow a hierarchy structure with CyberEvent as the base event and inherit any parent attributes. Events can be used to trigger interactions between objects in a simulation or used independently to affect entire scenarios.

Some examples of events available in Cyber DEM are:

- CyberAction - The fact or process of doing something, in or through cyberspace, typically to achieve an aim
- BlockTrafficEffect - Completely block all traffic over a communication channel
- CyberAcknowledge - Response to a CyberEvent that has requested an acknowledgment
- PhishingAttack - The fraudulent practice of sending messages purporting to be from reputable sources to induce individuals to reveal sensitive information or unknowingly initiate another attack

The full list is available within the Cyber DEM standard.

2.3 Cyber DEM BONES

Along with the Cyber DEM standard, there is a supplementary document available called Base Objects, Networks, Effects, & Specifications (BONES) [8]. This document gives more detail about the Cyber DEM standard, including objects, events, and data structures. The BONES document is useful for understanding how and when to use certain objects and events. It also gives use cases for working with the Cyber DEM standard.

3 Serapis Cyber DEM Implementation Project

As part of a Defence Science and Technology Laboratory (DSTL) research project (SSEAIIU47.5.36), Pitch Technologies Ltd investigated the extent of the standard's usefulness. The aim was to evaluate if the Cyber DEM standard provided enough resources and a well-defined architecture to create a simulation within the cyber domain. The task made use of both new and existing tools, with the results presented at a stakeholder demonstration event.

3.1 The aim

The project aimed to show how cyber effects can be represented in conjunction with other military domains to support defense training. This involved utilizing existing and emerging open standards, like Cyber DEM and High Level Architecture (HLA) [9].

In collaboration with the customer, Pitch developed a use case prior to any development taking place on the project. The chosen use case makes use of several cyber-attacks and cyber effects, which affect both a civilian population as well as a military C2 system.

There are two main parts to the use case; utilizing cyber-attacks to gain unauthorized access to the system, and causing negative cyber effects to an existing system.

The first part follows the path of a cyber-attacker trying to gain access to a system that can then be used to cause large-scale panic among a civilian population:

1. A cyber attacker sends a phishing email to employees at a government company. Through this phishing attack, the credentials of an employee are gained by the cyber attacker.

2. Using these credentials, the cyber attacker can log in to a government data center, impersonating the government employee.

3. Once logged into the data center, the cyber attacker can exfiltrate a list of usernames and passwords for other government services.

4. Using the exfiltrated usernames and passwords, the attacker can access the government text messaging service. This sends a global text to all civilians.

5. Using the global text messaging service, a malicious message is sent causing civilians to flee in panic

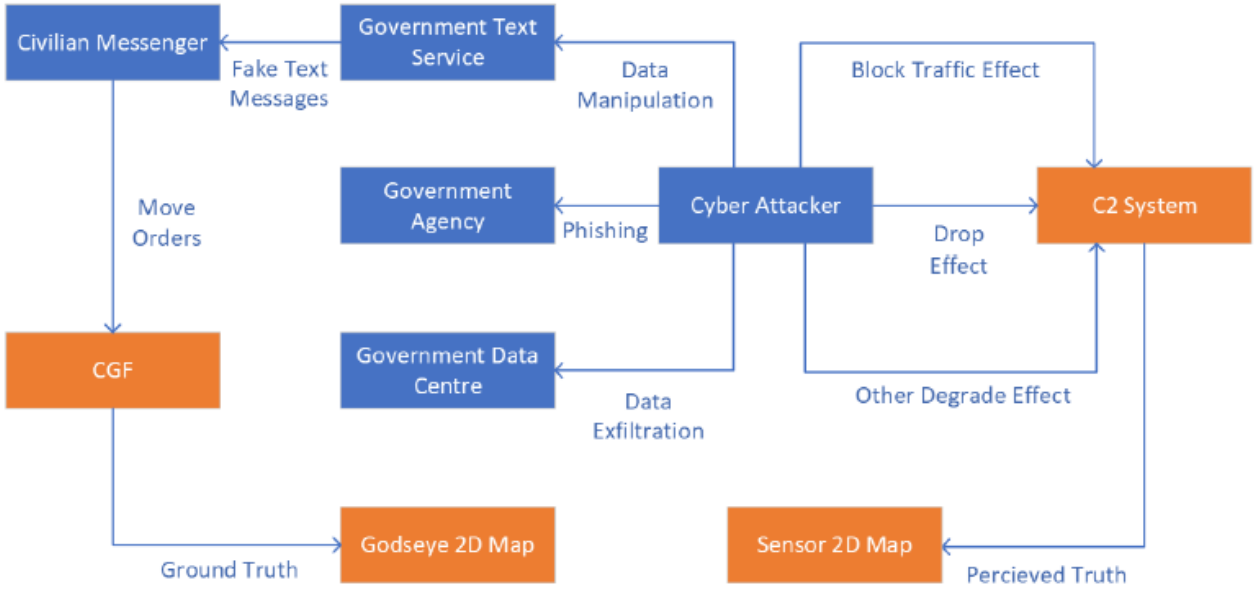


Figure 1. Cyber DEM Interactions

Concurrently, there is another cyber-attack taking place. This attack is targeting a military C2 system that is monitoring the situation caused by civilian panic. The C2 system then comes under several cyber-attacks, these include –

1. Block Traffic – This attack blocks a certain percentage of traffic from making it to the C2 system and for example, causing the C2 system to only display 50% of the entities that exist.
2. Drop Traffic – This attack blocks all traffic. This causes the C2 picture to stop updating. Unlike the block traffic attack, the entities will remain displayed but they will not receive any updates.

Both these sets of cyber-attacks look to disrupt and negatively affect civilian and military targets.

Having set these use cases, Cyber DEM would be implemented over several simulations. Making use of both cyber objects and events to evaluate whether the standard had enough detail and guidance to meet the aim.

3.2 Development

With the above aim, a development plan was created to achieve using cyber effects with a simulated environment.

High Level Architecture (HLA) was used as the interoperability backbone for the simulation, which meant using the Cyber DEM FOM. The Cyber DEM FOM is an interpreted version of the Cyber DEM objects and events into a Federation Object Model (FOM). A FOM is used in HLA to define the different object models and interactions used when simulation (Federates) communicate together in the simulation (Federation).

Another FOM that needed to be used within the simulation was the Real-Time Platform Reference FOM (RPR FOM) [10]. The RPR FOM is a SISO standard FOM that is heavily used within defense as it defines detailed objects and interactions that can be used to simulate most defense-based use cases. In this case, RPR FOM is used to define human objects to represent the civilian population.

As the goal was to create an effective distributed simulation, multiple federates needed to be created using both Cyber DEM FOM and RPR FOM. Figure 1 shows the overall Federation architecture, with orange federates being already existing systems and blue federations being new federates.

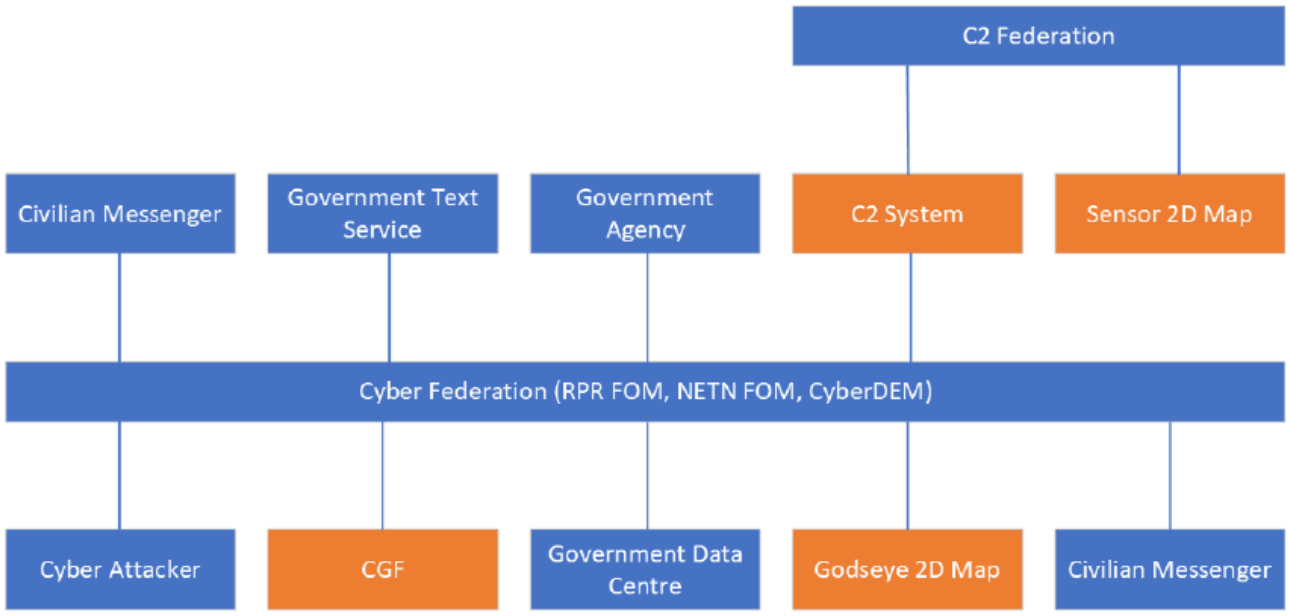


Figure 2- Federation Architecture

The overall simulation is split into two federations (Cyber Federation and C2 Federation). This is to allow for two C2 system map views; one that shows the ground truth, and one that shows the sensor picture. This enables viewers to see the effect a cyber-attack is having by comparing the two, as only the sensor picture is negatively affected.

3.2.1 Existing Federates

In this demo, there are several existing federates that required no development. These include –

- Pitch Actors – A basic CGF that reads a scenario file, using that to create, update, and delete entity object instances and interactions.
- Pitch Common Sim GUI – An interactive map used to display entity object instances.

- Pitch Extender – A tool to link federations together, and filter information based on several inputs.

3.2.2 New Federates

To simulate a mock cyber-attack, a network of linked systems needed to be created. As these systems would need to react to the Cyber DEM FOM objects and events, and there are no current systems that support this, they needed to be developed.

Development of these new federates was supported by the use of Pitch Developer Studio. This tool allows the user to generate middleware code based on any FOM. For this project, Developer Studio was given the Cyber DEM FOM, and generated Java code that was used as the base to develop the federates.

The new federates include –

- Civilian Messenger
- Government Text Service
- Government Agency
- Government Data Centre
- Cyber Attacker

Civilian Messenger
The Civilian Messenger is a console application using both Cyber DEM FOM and the NETN FOM. This allows the application to bridge the gap between the simulated cyber world and the simulated physical world. When the Civilian Messenger receives a valid text message from the Government Text Service it sends NATO tasking orders to the simulated civilian population, causing civilians to flee an incoming attack.

Government Text Service
The role of the Government Text Services is to act as a global messaging platform, allowing for messages to be sent to the phones of an entire civilian population. This is a console-based application using the Cyber DEM FOM, and more specifically reacting to the Manipulation cyber DEM event. If the correct login credentials are given in the Manipulation event, it allows the attacker to send a mass message to a civilian population.

Government Agency
A console-based application that acts as a simulated Government Agency or company. As an externally facing agency, it is susceptible to Phishing attacks. If the correct persona is the victim of a Phishing attack, then the application will provide the credentials needed to access the Government Data Centre.

Government Data Centre
The Government Data Centre represents a place where sensitive government information is stored. It is a console application that requires the user to log in to access any data. With the correct credentials, the user can access multiple pieces of data, one of these being a list of usernames and passwords for various government services. This data is published onto the HLA federation as data objects once the user is logged in. If an attack has gained access to the Government Data Centre it can then be susceptible to a Data Exfiltration attack, using the published data objects.

Cyber Attacker
The Cyber Attacker is a GUI-based application that is responsible for sending all Cyber DEM events in the form of HLA interactions. It also tracks all Cyber DEM FOM objects and interactions that have occurred while connected to the federation. Through the GUI, the cyber attacker can send all interactions defined in the Cyber DEM FOM, with access to all attributes as defined in the FOM. This allows for an attacker to simulate multiple different cyber-attacks with different parameters, to see how systems react.

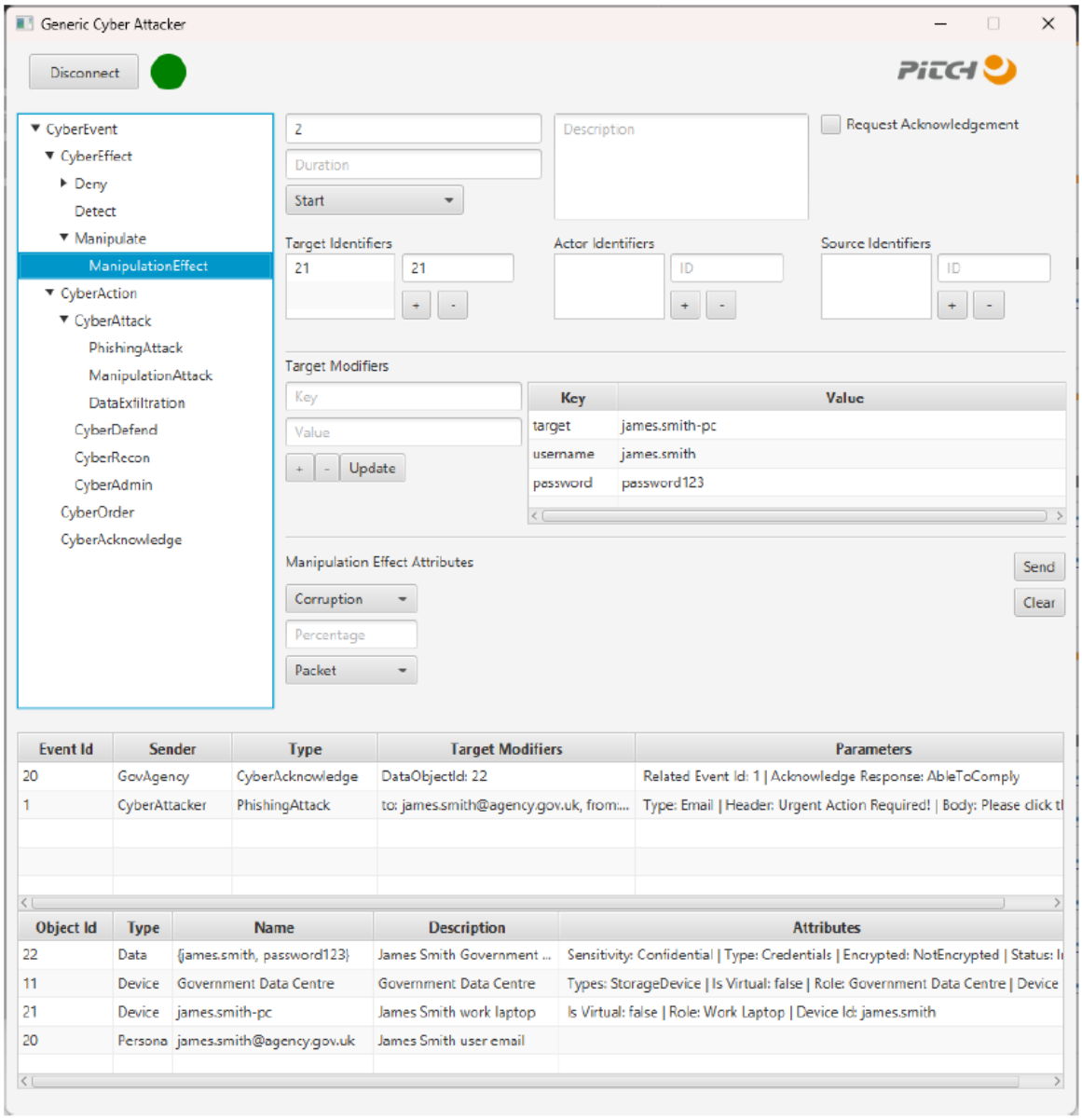


Figure 3- Generic Cyber Attacker GUI

Figure 3 shows the GUI used to interact with the cyber attacker.

The cyber attacker uses a separate configuration file to set several parameters. These parameters are used for connecting to specific HLA federations. Table 1 defines these parameters and what they do.

Configuration Setting	Usage
Federate Name	Name of the federate shown in the federation
Federation Name	Which federation to connect to
Address	The address of the RTI to connect to
Port	The port of the RTI to connect to
FOM	The FOM to use
Local Settings Designator (LSD)	Used to create one connection string instead of using individual values. If this is populated, all other connection settings are ignored

Table 1 - Cyber Attacks Configuration Parameters

Below is an example configuration file for the cyber attacker –

```
genericattacker : {
        connectionsettings : {
                federatename="CyberAttacker"
                federationname="CyberDemo"
                address="localhost"
                port="8989"
                fom="CyberDEMModule.xml"
                lsd=""
        }
}
```

3.2.3 Other Development

Apart from separate federations, a few other development tasks were needed to facilitate the use case.

Pitch Actors Scenario
A scenario file was created to define the number of civilians housed within a simulated village. These HLA entities could then be given movement orders as required.

Pitch Extender Filter Plugin
Pitch Extender allows custom filter plugins to be written and loaded at runtime. These filters can affect the data being transferred between federations. For this use case, a filter was created that listens for specific Cyber DEM interactions. Then when those interactions are received, depending on the interaction, the data packets are affected in some way. For example, if a Drop Traffic attack is detected, the filter stops all data flow until the drop time has passed.

This allows for one federation to have the "complete" ground truth, and another federation to show the cyber-attacked picture.

Due to using customizable filters, this has the effect of allowing the cyber-attacks to be carried out without changing the underlying simulation, both scenario and functionality. Instead of having to change the simulators, the data traveling between them can be changed.

3.3 The outcome

At the end of the development stage for this project, the results were several console applications, one GUI application, as well as scenario files and filter plugins. Using the applications produced it was possible to put together a demonstration rig that met the original use case.

3.3.1 The demonstration

One benefit of using HLA for the project is that it can easily run in a distributed architecture. To take advantage of this, and to strengthen the demonstration, three laptops were used in the demonstration rig. These laptops were connected on a LAN, with different parts of the demonstration running on separate machines.

This allowed one machine to act as the attacker, and the other two machines could host services used in the demo, for example, the Government Data Centre. The demonstration could then be run using the steps outlined above in the use case, showing how new and existing simulations could be cyber-attacked. By using HLA this could be distributed anywhere provided there is a network connection between the machines. It could also be run on one machine in a loosely coupled way, or each of the 10 federates could run on separate machines.

3.3.2 The Generic Cyber Attacker

The use case defined at the start of the project was very specific to a certain type of cyber-attack, whereas in reality there are many more types of cyber-attack and plenty of unused aspects in the Cyber DEM standard. The Cyber Attacker is generic to the Cyber DEM standard and can therefore be reused over multiple training scenarios. All attributes in the Cyber DEM standard are optional, meaning that the Cyber Attacker can be used to whichever fidelity suits the training need. For cyber defense training, low fidelity can be used to inform simulators that a certain attack has taken place and to react accordingly.

As a standalone GUI application, the Cyber Attacker is deployable to all environments and could be quickly implemented into an existing training system or used to help develop a new one.

3.4 Next steps

The work done as part of this project looked at a small subsection of objects and events that are defined within the Cyber DEM standard and simulated a specific use case. To take this further a larger, more generic, use case and scenario could be developed to make use of more features of the standard. Making use of more event attributes to enable deeper representations of cyber effects. Connection to cyber ranges could be a good start to achieving a larger scenario.

This could also include involving more human players, attackers, and defenders. The use case defined above for this project did not make use of the CyberDefend interactions at all. A red vs blue type scenario would show the usefulness of the standard and test the extent it can be used.

Another next step would be to integrate the Cyber DEM Standard into more existing simulation solutions. This would make it easier to set up larger-scale scenarios and involve more humans in the loop. In most cases, this would mean significant development effort to create plugins for these existing solutions.

4 Discussion

4.1 Experience Using the Cyber DEM Standard

At the start of the project, the risk was identified that the Cyber DEM standard might not support everything needed and that the data model might need to be extended. However, through our experimentation with the standard, we found that it fully supported what was needed to simulate the use case and demonstration.

Cyber DEM currently states that each attribute within an object or event should be considered optional. This provides users of the object model flexibility when defining their cyber simulations, however, it may lead to interoperability challenges when two different users of Cyber DEM attempt to integrate their simulations within a federation.

One example of where this flexibility may cause issues is that the identifiers of a Cyber Event are represented by an integer. However, there is no standardized method of assigning these identifiers, so they must be agreed upon and carefully assigned in a Federation Agreement; otherwise, identifiers may clash, leading to undefined behavior. An alternative method of identifying objects and interactions is using the NETN FOM [11] approach with Universally Unique Identifiers (UUID), guaranteeing uniqueness and removing this requirement from the federation agreement.

To enable almost all interactions, the TargetModifiers attribute is used to define the specifics of the Cyber Events in more detail than the object model allowed. The TargetModifiers attribute uses an array of key-value pairs. For example, the following TargetModifiers were used to interact with the text message service.

Key	**Value**
username	admin
password	abc123
textcontents	Ballistic Missile inbound to your area. Evacuate immediately

These TargetModifiers enable Cyber DEM to model a wide range of use cases, of varying fidelities, as any number of key pairs can be attached to a cyber-event. However, these TargetModifier keys must be agreed upon in a Federation Agreement to allow senders and receivers to know how to interpret them correctly. As the TargetModifiers are not standardized, it will make the reuse of components between different simulations difficult as interoperability challenges are likely to exist. For example, one simulation may have used a username field as key 'user' while another may have used 'credentials'. Semantically, these fields would mean the same thing. Still, they would not be understood

programmatically, leading to code changes to allow the correct interpretation of data.

Cyber DEM recommends that users follow the timestamping methodology implemented by a related kinetic simulation when timestamping Cyber Event messages. Furthermore, timestamping should be defined in the federation agreement if there is no related kinetic simulation. This design means that different Cyber DEM-based applications could represent time differently. Again, this would introduce a reuse challenge.

HLA FOMs require that a datatype's base encoding is defined in the object model, and the draft Cyber FOM sets the timestamp encoding to a signed integer. The Cyber DEM FOM notes state that this is a temporary definition that will be changed in the future to an unsigned integer, as per the DIS standard's [12] technique for representing time. The intent is that once HLA 4 is released, the new in-built signed integer type will be used. However, this would mean the FOM would not be backward compatible with the current HLA Evolved standard and could require two separate representations. Furthermore, the upcoming RPR-FOM v3.0 will potentially change the way messages are timestamped. It is worth noting that the Cyber DEM FOM is not part of the standard, which leaves the interpretation of the standard up to the FOM builders

4.2 Thoughts on the Cyber DEM Standard

Overall, the Cyber DEM provides an excellent high-level basis for starting to model Cyber effects in a standardized way. It also offers several customizable data fields that allow users to define and exchange data that goes beyond the scope of what Cyber DEM provides. However, when using these customizable fields, the data defined is not standardized. This lack of standardization will make any federate using these fields harder to reuse effectively.

However, if there is to be more standardization added to the customizable data fields this must be done carefully. If it becomes too standardized and defined there is the risk that the standard loses its flexibility and becomes difficult to work with. There is also the option to extend the object model based on more specific use cases. While this might work for use cases where the object model can be agreed between parties, it means that another third party might not be able to join the collective scenario as they are using the base standard without extension. This reduces the interoperability of the standard and goes against the point of publishing an agreed standard. The Cyber DEM standard is still under review and there have been several comments back to the working group, which might be incorporated in a future formal standard.

4.3 Use of the Cyber DEM Standard in the Cyber Domai

As it stands, a development effort would be required to integrate the Cyber DEM standard into the existing cyber domain. Not just for defense training but for other commercial domains as well. This project showed that the standard can be used to develop a demonstration in a relatively short time, a number of the applications were custom-made to meet the requirements. If the requirements were larger and more complex, then the development time of these custom applications also increases.

The use of HLA, while providing a backbone based on a well-established technology, does not guarantee fast interoperability in the entire cyber domain. While HLA is used extensively in defense, other domains like space and gaming are only just starting to adopt and use it. This brings more interoperability challenges that are not inherently something the Cyber DEM standard can do much about. However, as the standard is an ontology, it lends itself well to being implemented in all domains, using many different technologies.

5 Conclusion

Simulation of Cyber Effects has a wide range of use-cases and each of these use-cases would require different fidelities of simulated models to meet various training needs. This results in the requirements placed on the data model to be able to

accurately describe all the information required to simulate these effects being large.

Cyber DEM is an emerging standard that is seeking to be able to cover these wide-ranging use cases and as such the standard describes data from a high level. It provides a layer of flexibility by allowing a user to add custom data to objects and interactions allowing for more low-level detail to be covered. This flexibility comes at a cost, as it reduces the interoperability between devices and makes re-use difficult without code changes being made.

Cyber DEM was shown to support the requirements of our use case without the need for modification, although some design decisions had to be made that could break re-use. It was also able to co-exist with both RPR and NETN FOM with existing simulations being extended to add support.

Pending formal publication of the Cyber DEM standard, it is considered to be at a level of maturity for early adoption in defense training and experimentation. This early adoption should be done in a controlled manner with appropriate interoperability requirements and guidelines, to ensure a level of re-use and interoperability.

The Generic Cyber Attacker tool could provide a good base for other simulation systems to be built or improved to support the Cyber DEM standard on HLA. The usefulness of the other translations of the Cyber DEM standard was not assessed, but due to the nature of the standard being an ontology, assumptions can be made that they would have similar benefits and face similar re-use issues.

References

[1] Number of internet users worldwide from 2005 to 2022(in millions), https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

[2] NCSC Annual Review 2022, https://www.ncsc.gov.uk/collection/annual-review-2022

[3] NCSC Certified Training, https://www.ncsc.gov.uk/information/certified-training

[4] UK Defence cyber skills to be boosted through industry partnership, https://www.gov.uk/government/news/uk-defence-cyber-skills-to-be-boosted-through-industry-partnership

[5] Mitre Attack Matrix, https://attack.mitre.org/

[6] SISO Standards About Page, https://www.sisostandards.org/page/AboutSISO

[7] SISO-REF-072-202x Reference for Cyber Data Exchange Model (DEM) Product Development Group (PDG) Cyber DEM Base Objects, Networks, Effects, & Specifications (BONES), Cyber Data Exchange Model (DEM) Product Development Group, https://sisostandards.connectedcommunity.org/communities/community-home?CommunityKey=d888b620-620e-445d-81bf-f10a3aa1c3af&LibraryKey=0fd2382d-bffd-4baa-b2f6-bd503934a3e1

[8] SISO-REF-072-202x Reference for Cyber Data Exchange Model (DEM) Product Development Group (PDG) Cyber DEM Base Objects, Networks, Effects, & Specifications (BONES), Cyber Data Exchange Model (DEM) Product Development Group, https://higherlogicdownload.s3-external-1.amazonaws.com/SISOSTDS/f2bd8342-8e5f-d883-8002-b94826cb633d_file.pdf?AWSAccessKeyId=AKIAVRDO7IEREB57R7MT&Expires=16986689 16&Signature=2gYtCon0%2F8yD2TeHY3HCuDaw9k8%3D

[9] IEEE, "High Level Architecture for Modelling and Simulation," IEEE 1516-2010, 18 August 2010

[10] SISO-STD-001.1-2015: Standard for Real-time Platform Reference Federation Object Model (RPR FOM), Version 2.0, https://www.sisostandards.org/page/StandardsProducts

[11] NATO Education and Training Network Federation Object Model (NETN FOM), https://amsp-04.github.io

[12] IEEE Standard for Distributed Interactive Simulation--Application Protocols, https://standards.ieee.org/ieee/1278.1/4949/

Author Biographies

GARRATT WEBLIN is a Software Developer at Pitch Technologies UK focusing on open standards-based simulation interoperability for gaming technologies, cyber, and cross-domain security within defense, space, and other applications. Garratt is a key contributor to Pitch Technologies recent developments on projects across different domains working with novel technologies, integrated systems, and cyber. He studied BSc Computer Science at the Brunel University London.

JONATHAN DENNY is a Solution Architect at Pitch Technologies UK focusing on UK R&D projects. He has more than 10 years of experience in the design, development, integration, and acceptance of military training systems, with a focus on CGF and synthetic environments, for UK and international customers. Jonathan is also a senior member of Pitch's product development team and he studied BSc Computer Science at the University of the West of England.

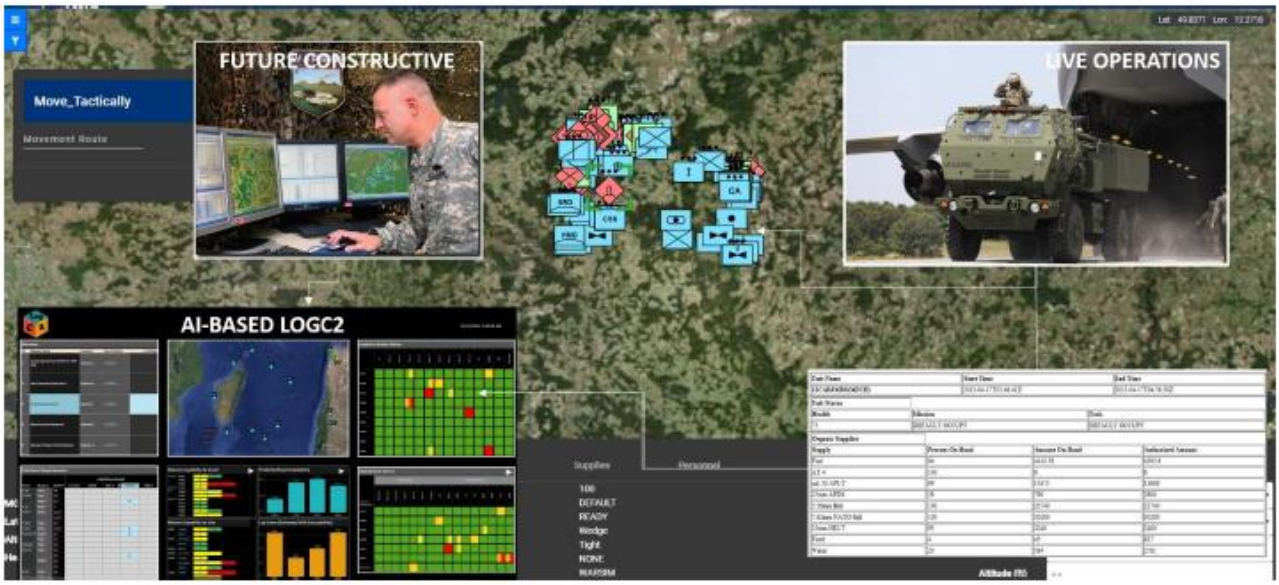
MATT TIPPER is a Software Developer at Pitch Technologies UK working with a focus on open standards-based simulation of voice and radio communications for defense training. Matt has recently been heavily involved in several research and development projects across different domains working with novel technologies, integrated systems, and cyber. He studied BSc Computer Science at the University of Birmingham.

AI-driven Logistics Intelligent Decision Support (A-LIDS)

Lockheed Martin – Rotary and Mission Systems (RMS)
Training & Logistics Solutions (TLS)
100 Global Innovation Circle, Orlando, FL, 32825

Primary POC: Robbie Phillips
Tel: +1 407 4622 783
Email: Robbie.phillips@lmco.com

Research Concept Whitepaper
This paper has been prepared for public dissemination by the NATO CA2X2 Forum.



1 Military Problem Statement

Providing continuous and timely sustainment to the force will become more challenging on the modern battlefield. Secure and reliable networks will pass data to allow sustainers to accurately monitor consumption of all classes of supply and conduct predictive analysis using AI, while robotic vehicles deliver diagnostic support to the point of need, enabling the Army, Joint, and Combined Force to continue combat operations with little or no delay. Additionally, medical providers must be able to anticipate the time and location that casualties will likely occur so critical treatment assets can be staged to facilitate the collection, triage, treatment, and evacuation of casualties.

Currently, during mission planning, operational commanders often do not have full awareness of platform readiness. As complexity of mission increases, so does the courses of actions (COA). Operational commanders are often tasked with assimilating multiple sources of information to decipher which COA is most viable. In addition, supply chains supporting joint operations do not always have full visibility of current and predicted mission needs. Thus, commanders often are not able to appropriately preposition assets where needed. In summary, there is a recognized need for next generation automated Sustainment Decision Support.

2 Technology Description

Our approach will focus on the development and refinement of an AI-driven Logistics Intelligent Decision Support (A-LIDS) system shown at the center of Figure 1.

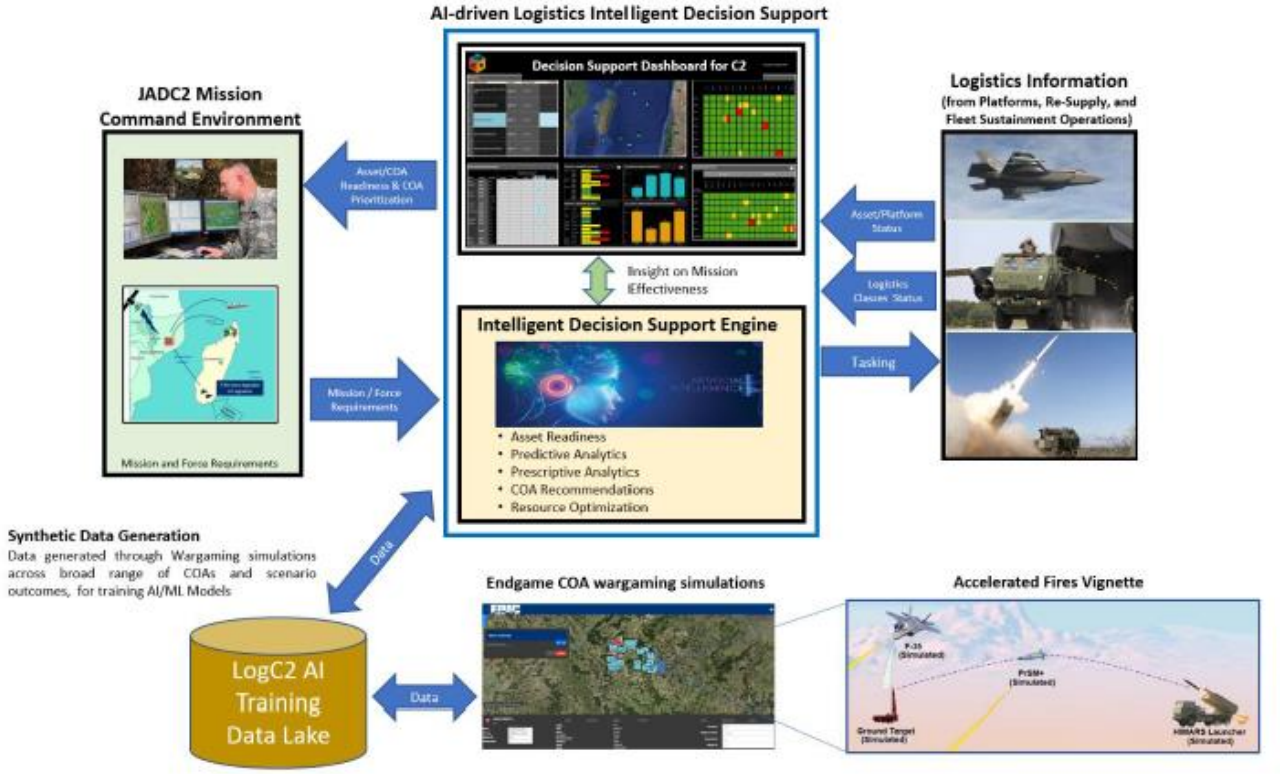


Figure 1 – AI-driven Logistics Intelligent Decision Support (A-LIDS) System Architecture

To build training models accurately and effectively, there is a definite need for data encompassing potentials scenarios and outcomes. In the absence of real-world operational data for the future fight, we plan to leverage synthetic data generated using a suite of simulation tools Lockheed Martin is investigating for a Future Constructive simulation capability.

This evolving collection of simulation tools are identified by Lockheed Martin as Endgame, which consists of;

1) Army validated Warfighter Simulation (WARSIM) to represent the ground maneuver and combat, and combat support of future Army force structures,

2) web-based interface for the Battle Staff Trainer (EPIC) to plan, prepare, execute and assess scenarios and Order of Battle (ORBAT)

3) high fidelity engineering models for key enabling platforms for future accelerated fires scenarios (such as the F-35, PrSM, and HIMARS), as add-ons to WARSIM or the simulation environment

Leveraging Endgame for synthetic data generation will allow training of AI models in A-LIDS to provide intelligent decision support services such as predictive and prescriptive logistics recommendations, projected asset readiness, and course of action confidence ratings. Endgame will be used for modeling mission scenario execution as well as generating the logistic information reports and combat unit assessments such as

attrition, casualty assessment, asset failures and repair delays for a range of specific simulation runs based on identified Courses Of Action.

The Training Data Lake will be generated over multiple (hundreds or thousands of) simulation runs in order to provide a meaningful dataset upon which to train AI models. Specific measures and rule sets will be utilized to train the initial models through supervised and unsupervised learning techniques, benchmarked against minimum confidence levels. Once trained, the models will be converted to a number of LogC2 decision support services within an Intelligent Decision Support Engine, to be tested in a simulated decision environment. Lockheed Martin will request the participation of Army Logistics subject matter experts to participate in the desktop analysis of both measures and verification testing. Once the rule sets and confidence levels are verified, the A-LIDS Decision Support Dashboard will be used to validate the effectiveness of A-LIDS against sample scenarios. Ultimately (and if successful), we envisage A-LIDS ingesting real time situational awareness and joint logistics posture to continuously provide accurate sustainment decision support and recommend the best course of action that is most logistically sound.

3 Concept of Employment

This project will focus on the ability to access and intelligently fuse data from multiple sources (supply chain, personnel, maintenance, equipment status, etc.) real or synthetic to provide situational awareness, decision making, and predictive intelligence based on logistics and sustainment postures. The demonstration focuses on the ability to link the data sources and decision tools to provide Logistics Command and Control "speed of relevance" insights to aid commanders and staff to take better decisions in a contested environment.

Our goal for the A-LIDS System to provide actionable situational awareness for the Joint all-domain operation commanders. A few examples are as follows:

- Theater-wide knowledge of current and projected Asset readiness and logistics posture

- Integration with the Commander's C2 to inform/enlighten combat operations

- Operational/strategic level maintenance decisions to maintain or restore combat readiness

- Forecast sustainment needs to maintain/anticipate operational pace

- Dynamically position inventories to minimize response times and minimize/reduce risk

- Plan intra-theater transportation and distribution

Consolidating these and related capabilities in support of JADC2 is a challenging endeavor. For purpose of the Project Convergence 22, we will focus on testing, integrating, and demonstrating novel AI-based capabilities of Logistics Intelligence Decision Support that fuses and matches predictive asset readiness & availability to evolving mission needs. The next few paragraphs briefly introduce the visualization concepts to be tested and then explains the underlying asset to mission matching.

A-LIDS Dashboard: As previously mentioned, A-LIDS strives to provide insight about the current and future readiness of key military equipment relative to evolving mission intent. Figure 2 illustrates an aspect of the insight visualization concept we want to provide in contested logistics scenarios. The Dashboard would allow commanders to see current and predicted readiness of forces at multiple echelons – COA readiness, Asset readiness, Logistics class readiness and Parts availability. It would also provide commanders with various types of COA analysis such as (a) Current status and locations

of assets needed by the COAs (b) Predicted time when all assets needed by a COA will be ready to engage (c) Logistic impact of running a COA on logistics classes including supply, fuel, manning (d) Provide a time sensitive Logistics score for each COA that reflects its viability of a logistics point of view, taking into account the status of logistics classes and predicted readiness of assets.

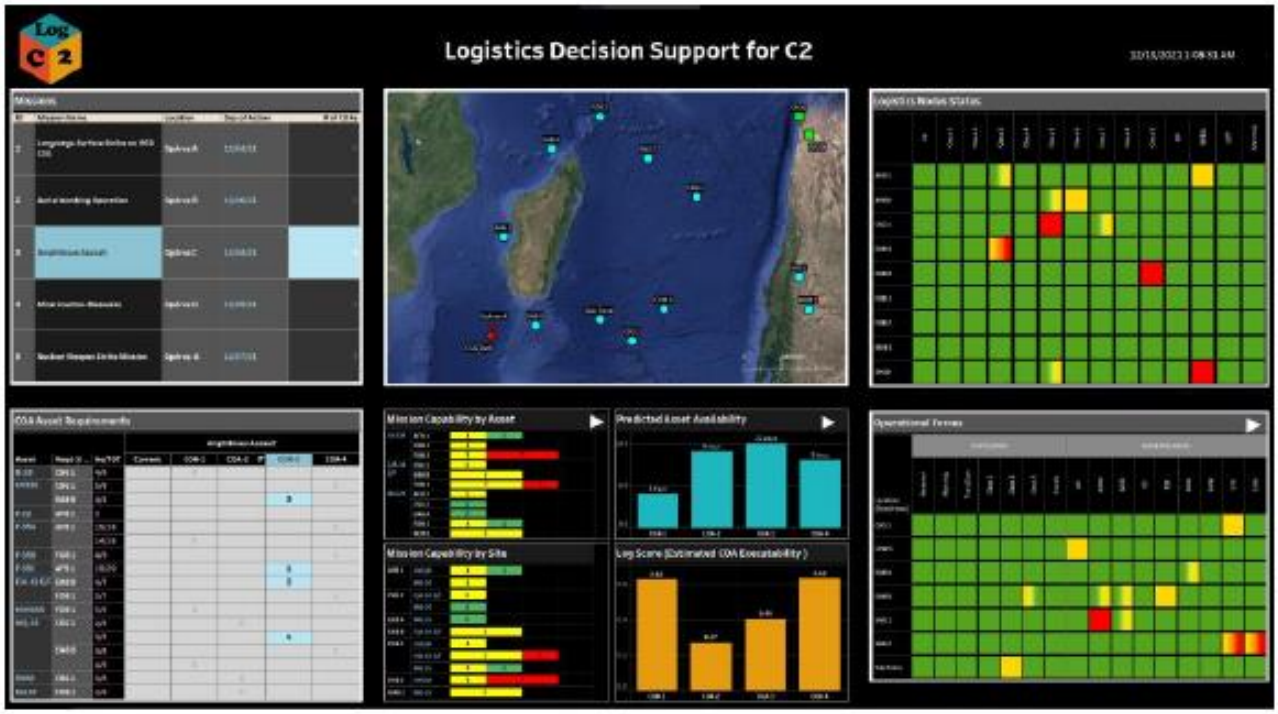


Figure 2 – Prototype A-LIDS Dashboard that provides decision support

Asset Readiness Prediction: Obtaining an accurate estimate of current equipment readiness is a technical challenge alone because mission readiness can be driven by supply or maintenance issues and future readiness requires predictive modeling of both equipment and logistics/supply chain health. A contested logistics environment additionally challenges the efficacy and resiliency in the predictions to evolving mission matching. Figure 3 shows a prototype instance of the Readiness Prediction within A-LIDS for a Sikorsky rotorcraft that is predicting unscheduled maintenance drivers within a time horizon based on estimated future usage (e.g. mission type) so the aircraft with the highest readiness for the mission can be selected or targeted mitigating action can be prioritized. This prediction is accomplished with a fusion of dynamic Neural Network-based classifiers and survival models at the key component level. If near real-time equipment health data (e.g. fault codes) or future mission types change, the estimates change accordingly.

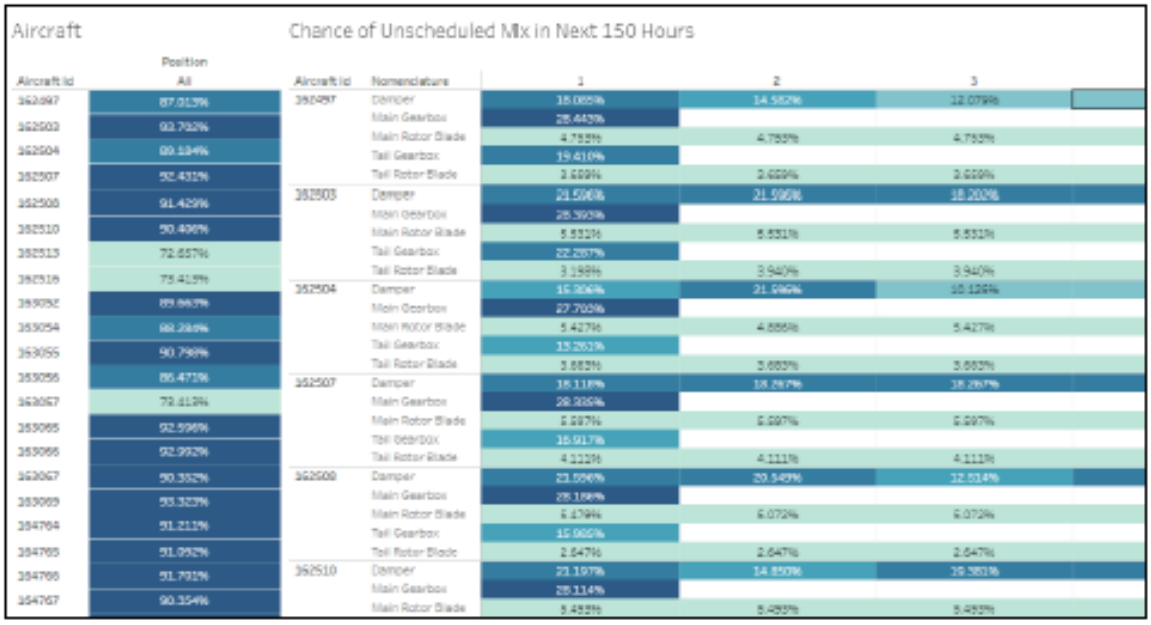


Figure 3. Asset Readiness Prediction

Parts Survivability Analysis: We will also leverage one of our recent IRAD on Predictive AI for Supply and Sustainment to accurately predict parts demand, so that Operational commanders can preposition the right parts in the right place at the right time. This IRAD focused on using Machine Learning models and Statistical algorithms for predicting parts survivability while taking into account several operational and weather factors that may have had an impact on the part's life. We were able to demonstrate the variability of survival curves under the influence of varying operational and weather conditions. We plan to leverage this work and extend it to predicting part demands in a contested environment.

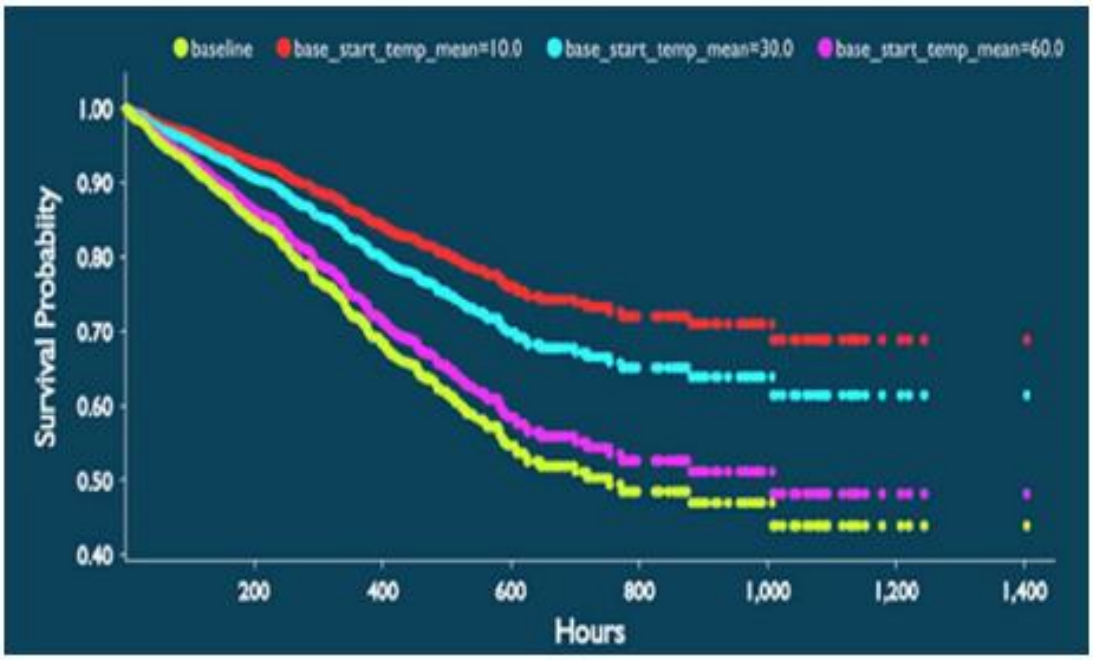


Figure 4. Effect of varying temperature on Survival Curves

Synthetic Data Generation using Endgame: These capabilities will require a significant amount of data to demonstrate their full potential. Endgame includes WARSIM which will be used to augment real platform and logistics data to help introduce additional scenarios and constraints that could result in alternate logistic courses of action. WARSIM's unique aggregate-entity design provides the detailed modeling down to the individual vehicle level necessary to train the Commander and staff while providing the aggregate-level modeling for larger Brigade and Division scenarios (Figure 5).

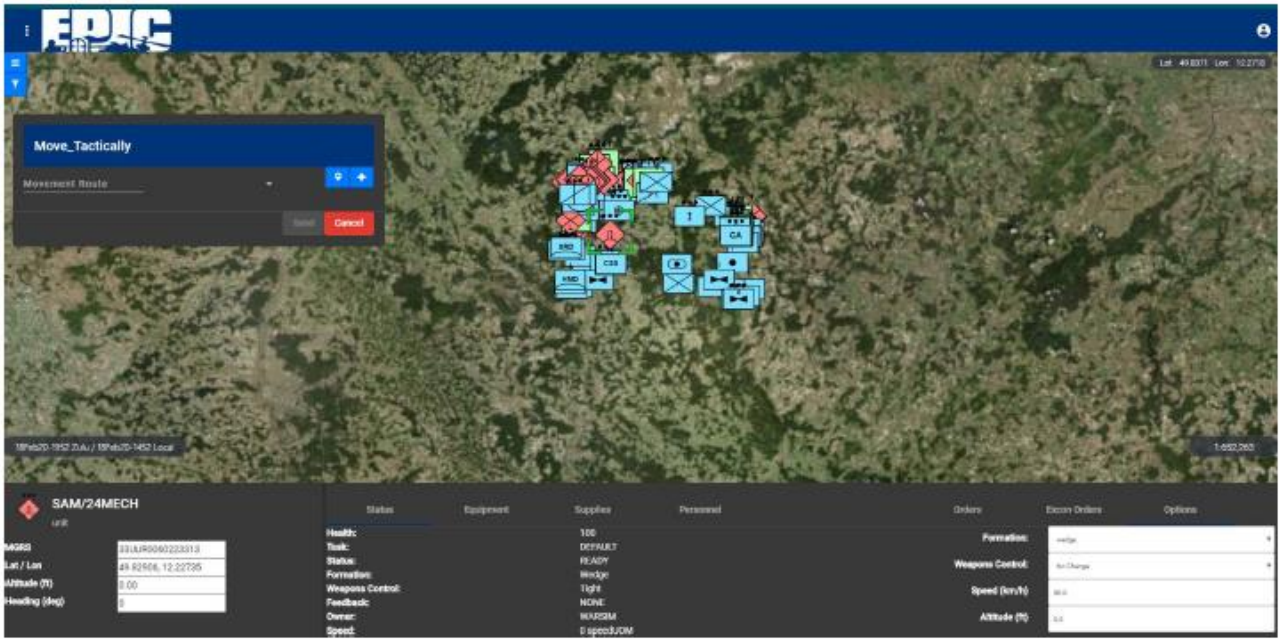


Figure 5. ENDGAME will be based on Army validated models of WARSIM and the EPIC User Interface

WARSIM also models supply of food, water, fuel, engineering supplies, ammunition, major end items (platforms), medical treatment supplies, and maintenance repair parts. Supplies are explicitly tracked and can be loaded on transports, moved on transports, unloaded, established in caches, and consumed. Supplies are subject to attrition based on their actual location (what platform they were loaded on). Damage can be increased with the attrition of fuel or ammunition. Personnel are loaded, transported, and unloaded on specific platforms for the purposes of transportation. All these capabilities allow detailed tracking of who and what are on all the transports in the battlespace, allowing detailed logistics tracking.

In addition, this level of detail allows the WARSIM model to be easily linked to detailed entity level models representing future fighting capabilities. Lockheed Martin has more specific engineering models and simulations which represent air and surface assets.

4 Technology Maturity

The current decision tool framework and tools that will be used for A-LIDS are TRL 4 and have been developed under Lockheed Martin IRAD projects such as JADO BMC2 (Battle Management Command and Control) to support Log C2 capability integration with JADO modeling. We will also be leveraging a recent IRAD on Predictive AI for Supply and Sustainment. This IRAD attained TRL 6. Endgame includes WARSIM and EPIC which are currently fielded for battle staff training globally (TRL 10). WARSIM which has been the backbone of single service and Joint constructive simulation exercises and experiments for more than 15 years.

5 Multi-Domain Operational Environment

Mission Thread: Conduct Joint Sustainment Operations

The mission thread will include US Army, US Air Force, US Marine Corps, and Coalition partner (Australian Army) components participating in simulated Joint Sustainment Operations, providing combat support including resupply.

Use Case: Sustain Dispersed Forces Along LOCs in Contested Environment

The use case will incorporate a strategic fires battalion employing advanced warfighting capabilities such as PrSM employed against a near peer threat.

Figure 6. Engagement Scenario: Dynamic Sustainment Support to Accelerated Fires (Army G-4 / JHU APL)

The engagement scenario will consist of supporting fires to Coalition ground forces, utilizing Joint assets to perform both targeting and resupply tasks. The scenario will include the option to conduct manned and/or unmanned resupply operations.

+ Area of Influence:

The A-LIDS experiment will focus on elements of combat support across all three areas;

- Strategic Support Area
- Operational Support Area
- Tactical Support Area

+ MDO phase supported:

The mission thread is relevant to all MDO phases of operation;

- Compete
- Penetrate
- Disintegrate
- Exploit

+ MDO Tasks addressed:

While the accelerated fires scenarios will incorporate many or all of the MDO tasks;

- Stimulate
- See
- Strike
- Move
- Communicate
- Decide
- Sustain

the objective of the A-LIDS experiment is to investigate the suitability of this technology to enhancing Decide and Sustain tasks.

Kubernetes as a SimaaS Platform

Utilizing Containerization for Simulation Workloads

Daniel Seufferth, daniel.seufferth@unibw.de,
Heiderose Stein, heiderose.stein@unibw.de,
Falk Stefan Pappert, falk.pappert@unibw.de,
Oliver Rose, oliver.rose@unibw.de

Universität der Bundeswehr, Neubiberg (Germany)

Abstract

Kubernetes is a cornerstone of the modern microservice-based internet. Various service providers – like Spotify, Netflix, etc. – use Kubernetes to distribute their workload and ensure a high availability of their services. Leveraging the capabilities of Kubernetes and containerization is the obvious step for creating a scalable and highly available Simulation-as-a-Service (SimaaS) platform. This paper discusses the different aspects and difficulties of using containerization for simulation workloads, which must be considered. Furthermore, it describes the setup of the SimaaS-cluster of the University of the Bundeswehr Munich and shows the first results of performance gain based on an example of a manufacturing simulation application.

1 Introduction

Computational power is a limiting factor for simulation. Over the past decades, the increasing performance of personal computer hardware allowed the execution of simulation experiments using single PCs. When the complexity of one single simulation run – or the sheer number of simulation experiments as in data farming or simulation optimization (Lechler et al. 2021) – exceeds the capacity of a single PC (see Sanchez et al. 2021), there is a need to use more powerful computing systems (Król et al. 2013) as an environment for running simulations.

2 Requirements for using containerization for simulation at scale

Three key aspects are required to efficiently use Kubernetes and containers as a SimaaS platform. First, knowledge about both technologies, Kubernetes and containerization. Second hardware, on which you can set up Kubernetes and run containerized simulations. Third, simulation-specific requirements. We discuss these three aspects in more detail in the following sections.

Due to the rise of cyber interactions and the significant increase of research into cyber training throughout academia and industry, a SISO Product Development Group (PDG) was created and tasked with identifying key cyber activities, and lessons learned, and evaluating potential standardization areas within cyber modeling and simulation.

2.1 Knowledge

Naturally, using a tool requires knowledge, which is also the case for containers and Kubernetes. (Huawei Technologies Co. Ltd. 2023) summarises the evolution of containerization, beginning with the chroot-command and finishing with modern containerization formats like Docker or LXC. Hitchcock 2022 describes the core concepts of containers and compares them to a more well-known technology: virtual machines (VM). Furthermore, he explains in detail how to containerize code and lists best practices in container usage. This basic knowledge of container technology and how to containerize software is sufficient for containerized simulation experiments.

For Kubernetes, there are two topics for which you need knowledge: first, a general overview on how Kubernetes can be used to orchestrate containers efficiently. Poulton and Joglekar 2022 comprehensively summarize Kubernetes and its different capabilities. Second, the different methods available to create a Kubernetes cluster. Various resources on creating Kubernetes clusters can be

found on the internet. As a starting point, we provide an overview of popular tools for cluster creation.

Tool	Description
kubeadm	Kubernetes' most fundamental setup tools to create (minimum viable) clusters.
Docker Desktop	Besides providing the Docker container runtime, Docker Desktop also offers a Kubernetes mode, to create a one-node cluster.
minikube	A lean tool that creates a local one-node cluster on various operating systems where it is installed.
MicroK8s	A tool like minikube, developed by Canonical.
Rancher	The most sophisticated tool of this list provides a comfortable GUI to create scalable Kubernetes clusters. This is also the tool we used for our simulation cluster.
Hosted Kubernetes	As Kubernetes is the de-facto standard of web applications, every major cloud provider offers a hosted Kubernetes solution, e.g., Google Kubernetes Engine, Microsoft Azure Kubernetes Service, Amazon Elastic Kubernetes Service, etc.

Table 1: Overview of popular tools for Kubernetes cluster creation.

2.2 Hardware

Running Kubernetes requires some kind of computing infrastructure. Using a hosted Kubernetes service has the advantage of bundling hardware costs and cluster service fees and externalize service and administrative expenses, making this one of the most comfortable, yet costly, options. Alternatively, using VMs provisioned by your cloud supplier is also possible if you already use hosted cloud services.

Nonetheless, it is worth noting that the use of cloud resources may not be suitable for every use case, making private hardware or clouds necessary. As Kubernetes only has moderate hardware requirements, i.e., 2 GB of random-access memory (RAM) and 2 central processing units (CPU) per node, clusters can be generated on manifold configurations. A few hardware examples are edge/internet-of-things devices, office notebooks, desktop PCs, or even high-performance computers. Tools like the previously mentioned minikube or MicroK8s also provide a quick and easy-to-set-up Kubernetes cluster for first experimentations on a single machine.

2.3 Simulation-specific requirements

During our first experimentations with containerization and running containerized simulation workloads in Kubernetes, we found three requirements for effectively utilizing containerization for distributed simulation, which are visualized in Figure 1.

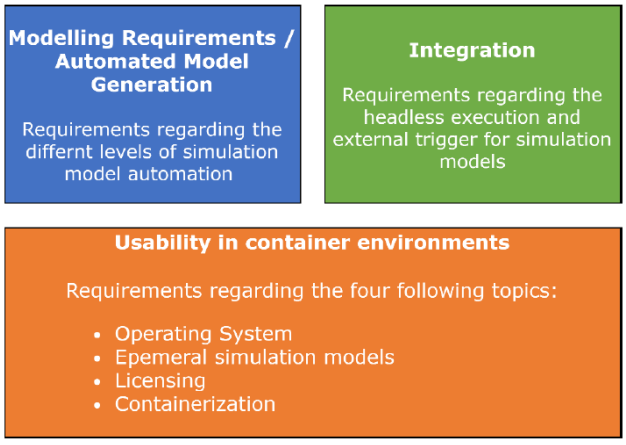


Figure 1: Requirements for simulation container.

We want to focus on the point of usability in container environments and will therefore discuss the four listed points in the following sections in more detail.

2.3.1 Operating system

As mentioned previously, containers are a form of OS (operating system) virtualization and use the kernel of the host OS. Therefore, Linux-based containers can only run on Linux machines. This means that the simulation model to be containerized must run on Linux. As only some engines support Linux, this restricts the number of simulation engines that can be used for model creation. Moreover, Kubernetes is designed to work with Linux containers. Architecturally the control plane, i.e., the management layer of Kubernetes, is required to run only on Linux hosts (Kubernetes 2023).

On the other hand, containerized simulation engines requiring Windows can only run inside a Windows container. To have Windows containers run on Kubernetes, a hybrid cluster, consisting of both Linux and Windows nodes, is necessary. A hybrid configuration of Kubernetes generates a performance loss, as it is no longer possible to allocate all the available resources when nodes of several operating systems need to be provided. This mix of systems increases the complexity of resource allocation. A way to circumvent the usage of hybrid Kubernetes clusters would be the usage of Software like Wine: this kind of Software allows (simulation) software developed for Windows run on Linux.

Table 2 gives a small overview of different simulation tools we have used for various purposes (discrete event simulation, fluid simulation, etc.) and whether they support Linux. This shows that although Linux support is not an exception, some (popular) simulation tools require Windows.

Simulation tool	Linux support?
Anylogic	Yes
Factory Explorer	No (Windows only)
Flexsim	No (Windows only)
Matlab/Simulink	Yes
OpenModelica	Yes
Simio	No (Windows only)

Table 2: List of simulation tools and the support of Linux-based OSs.

2.3.2 Ephemeral simulation models

As a container orchestrator, Kubernetes aims to have all containers running. In case a container fails, Kubernetes automatically restarts it as a new instance, possibly on a different worker node. This characteristic of containers in Kubernetes is called ephemeral, meaning they can get destroyed and restarted by the control plane at any given time due to internal or external causes. The causes of container deletion are various. Some common causes are, e.g., software updates, load balancing or, in the case of using Kubernetes as a SimaaS platform, simulation failures. Simulation models that run as containers in Kubernetes should therefore support this ephemeral nature. This gets especially important, when you run multiple instances of simulation models as different scenarios. We want to give a few ideas on how to handle simulation in such an environment: one way of handling the ephemeral nature of containers inside Kubernetes is accepting the killing of execution runs and restarting it. This brings the question of monitoring lost simulation runs. Kubernetes has several extensions that provide extensible monitoring and logging features, which can be used to keep track of prematurely stopped scenario calculations.

Another possibility of handling preterm destroyed containers would be to keep track of, and store, the progress of simulation runs. A kind of "checkpoint" system would make the restart of killed instances of a specific scenario without data loss possible. Such a mechanism would theoretically be possible, by utilizing a specific Kubernetes object that provides persistent storage to a container. However, keeping

an up-to-date image of the current simulation state in storage requires a significant amount of data. "Caching" large amounts of data, requires also continuous transfer from the container to the storage, possibly stalling other data transfers. In addition to the adverse effects on simulation speed and general performance, the general cost of storing is also an aspect to be considered. Therefore, this approach is only feasible in an environment where successfully finishing simulation runs is otherwise unlikely due to very long simulation runs or unstable computing hardware.

One last way we want to introduce is starting additional instances, adding redundancy, and decreasing the risk of data loss in case of a container failure. As most simulations already utilize replications to achieve sufficient confidence intervals, adding additional runs depending on stability would not increase the load by a large margin. This is also the method we choose for our first simulation experiments.

Using containerization technologies for simulating models at scale brings with it the need to consider the premature termination of simulation containers. This affects the number of simulation runs that can be completed. Furthermore, it requires consideration of the data collected during one run. While simulation models that purely run in memory usually leave no trace when their surrounding container disappears, simulation models reporting data during the simulation run to a database require more involved handling as incomplete data needs to be cleaned in case the container fails.

2.3.3 Licensing problems

Running multiple instances of a simulation model also requires multiple instances of the simulation software used. Therefore, for commercial simulation packages, the software vendors' approach to licensing is worth considering. The cost structure is one of the most important aspects to be reviewed when taking licensing into account. There are simulation packages where costs depend only on the model development environment. This allows very flexible scaling of the simulation to new or different projects. Then there are per-user/seat licenses, which can be challenging to scale in a legally safe way. A third option is a licensing model, which charges per core, which can get expensive when sufficient hardware is available.

Another side to licensing, besides the cost and legality, is the way the developer enforces licensing. From our point of view, licensing servers with concurrent licensing are ideal for a dynamic environment like Kubernetes. Any licensing scheme enforced by hardware restrictions significantly limits its use in a container environment. Examples are license codes tailored to a specific PC or hardware keys provided as USB dongles.

2.3.4 Containerization

Creating container images depends on the choice of the container engine. Multiple engines like Docker (Docker Inc. 2023), Podman (Podman 2023), or Apptainer (Apptainer Project 2023) are available, all of which have a similar approach to image creation, utilizing a descriptive file that defines all steps necessary for containerization, which we will call the "containerization file" in the following.

The containerization file generally begins with a base image, e.g., an Alpine Linux image, and defines which libraries and binaries to add. In the case of a simulation model, you need to package your simulation tool of choice, so the simulation engine is available inside the container. Supporting installation via the command line, containerization of the chosen simulation tools is done by adding a single command to the containerization file. If this simple installation method via the command line is not supported, a more tedious approach must be utilized for installing the simulation tool.

A wholly optimized containerization process for simulation models means that simulation package developers provide usable images of their simulation software, streamlining the containerization process of simulation models.

In a perfect world, simulation software developers would provide a secure base image of their simulation package, where the user only needs to add their model.

3 Kubernetes based simulation cluster

In the following sections we discuss the current architecture of our simulation cluster and how we plan to change this architecture in the future.

3.1 Current setup at the University of the Bundeswehr Munich

The current setup of the simulation cluster at UniBw Munich consists of two server racks, each of which contains 1280 CPU cores, 40 TB of RAM, and 20 TB of shared mass storage. Built on this hardware, we first created our Cluster Management Server, supported by Rancher, an open-source software and part of SUSE (see Table…). We use Rancher for cluster creation and management, as it allows a reproducible and flexible Kubernetes cluster setup. The Rancher container itself runs in a small Kubernetes cluster, built with three control plane VMs and worker VMs to ensure high availability.

The Kubernetes cluster used for our first experiments consists of seven VMs, again three control plane VMs and four worker VMs, on which the simulations are executed. The detailed architecture of the cluster is visualized in Figure 1. Each host has 64 physical cores and 128 logical CPUs (LCPU). The four-worker node VMs have 60 virtual CPUs (vCPU) and 1 TB of virtual RAM (vRAM) and are distributed on four host computers. The three control plane VMs have six vCPUs and 6 GB of vRAM allocated and run on one shared host computer.

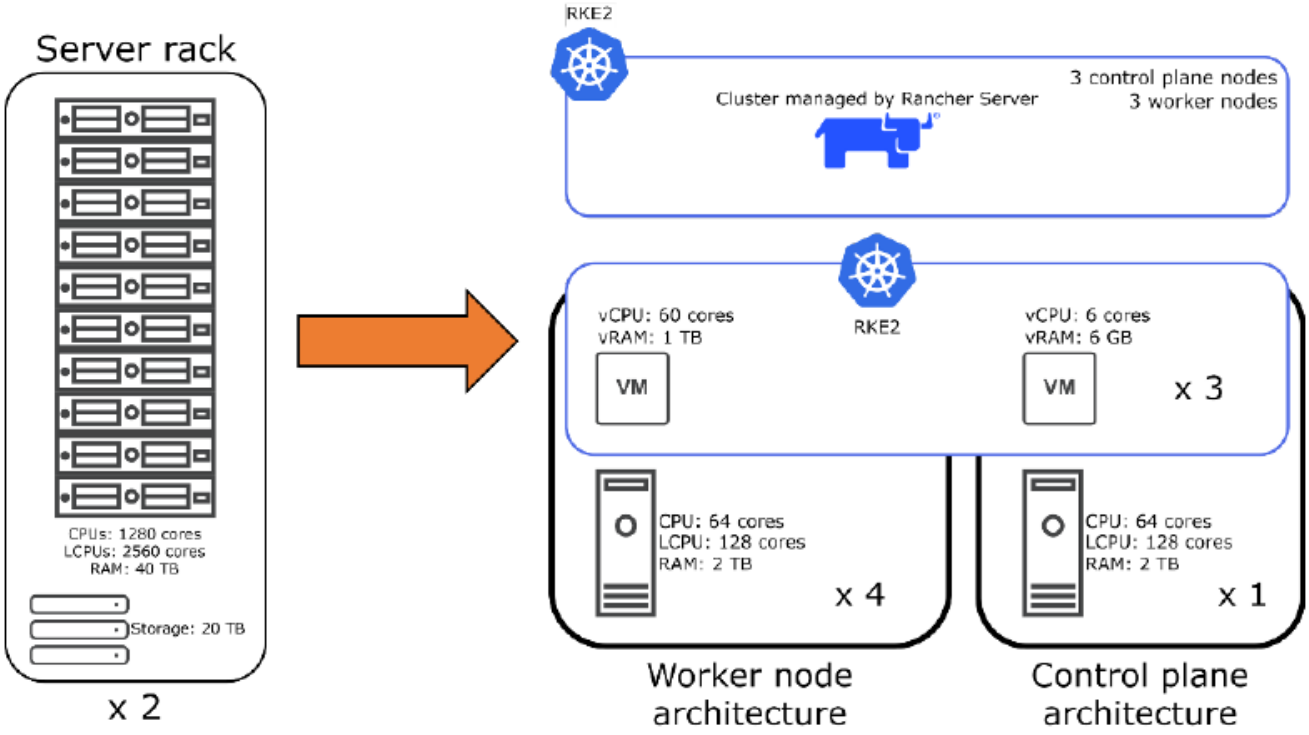


Figure 2: The current setup of our simulation Kubernetes cluster, consisting of three control plane VMs and four worker VMs.

3.2 Future architecture of the simulation cluster

The current architecture utilizes approximately 16% of the available computing power, hence we will extend the simulation cluster in the future. The control plane will still consist of three VM nodes but will be distributed on three of the 40 available host computers. This further increases the availability of our simulation cluster. The allocated resources of

the control plane VMs (6 GB of RAM and 6 vCPUs) will not change. We distribute the control plane VMs on three host computers. As the VMs do not consume all the hosts' computing resources, the free capacities can be used for other purposes, e.g., conventional VMs. In addition to the free computing power of the control plane hosts, we reserve three additional hosts completely for conventional VMs. Furthermore, one host will remain empty, for maintenance purposes. As the Rancher Server Cluster runs also on three hosts, ten of the 40 available host computers, will be reserved for different purposes. This leaves 30 hosts that are utilized for the worker node VMs, a considerable increase to the current test architecture. Besides increasing the number of worker nodes, we will also change the resource distribution of the worker node VMs, so that they can be separated into the following three different groups:

• RAM-tier: worker node VMs have 40 vCPUs and 1.5 TB RAM allocated.

• CPU-tier: worker node VMs have 80 vCPUs and 512 GB RAM allocated.

• Standard-tier: worker node VMs have 60 vCPUs and 1 TB RAM allocated.

These three tiers allow us to streamline the deployment of simulation containers based on the resource requirements of the model. As our Kubernetes cluster is used as a SimaaS platform, a multitude of simulation models are expected to run on it. From our experience, we know that some experiments require an increased number of RAM, which can be served through the RAM-tier. Model scenarios, that require less RAM can either run on the standard-tier or can be even more accelerated when utilizing the CPU-tier. Figure 3 gives a detailed picture of the planned future architecture of our SimaaS cluster and how we implement the different worker node tiers.

In addition to a more streamlined deployment process, this configuration makes the maintenance of the individual host easier. To perform hardware and software maintenance on one host, it is necessary to move every VM that runs on this host from it. Through the three different tiers, we achieve a distribution of hardware resources, which makes moving the VMs to different hosts easier. With an architecture that is planned with free computing power (i.e., one host for maintenance plus various not fully utilized hosts), moving VMs from one host to another can easily be done without performance losses.

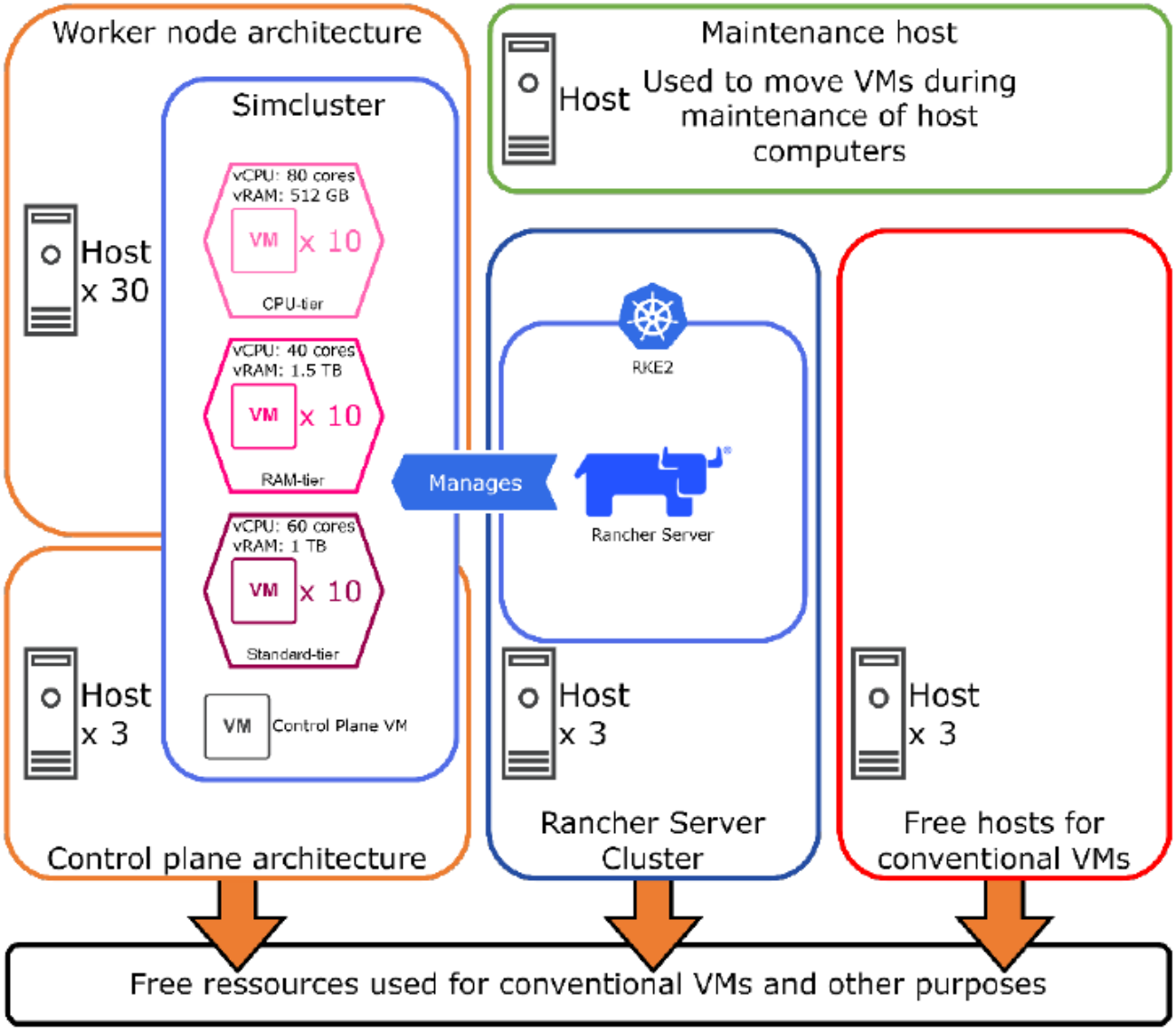


Figure 3: Future architecture of our simulation cluster.

4 First experimental results

The first test case run on our current simulation cluster is based on our work on utilization thresholds for equipment groups described in (Pappert et al. 2017). Here we use an in-house developed simulation engine, written in Java. The models are being created by simply calling methods of the meta-model. Furthermore, the experiment engine was designed with distributed execution in mind, meeting many of the requirements for utilizing containerization mentioned above. All this made the containerization process straightforward, only needing an image that includes the Java Runtime Environment.

With our historical changes to the computational infrastructure used, we can retrace the performance gain achieved by utilizing different setups, finally leading to containerization and Kubernetes. Figure 4 visualizes the performance – measured by the number of scenarios evaluated per day – based on the computational infrastructure. The shown configurations use different underlying hardware; therefore, the depicted performance gain of using Kubernetes can primarily be attributed to the extension of the hardware resources. The last two entries show our current simulation platform in two different scaling levels. The primary benefit we see in using Kubernetes comes with its ease of scaling. Once a small cluster is set up on a

small portion of hardware, scaling available processing power to full capacity is a matter of a few minutes.

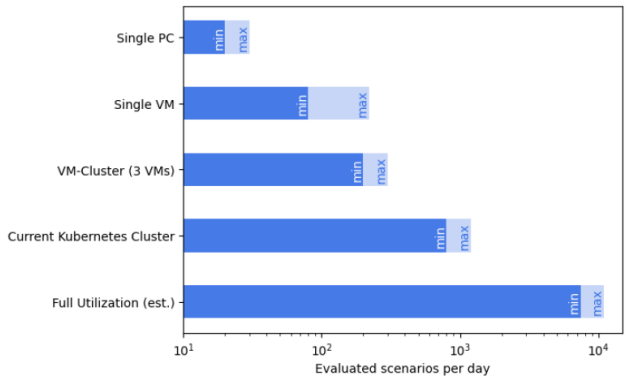


Figure 4: Performance comparison based on different computational infrastructures shows the number of scenarios calculated daily for each setup.

5 Summary and next steps

Our first experiments showed how Kubernetes allows us to utilize the server infrastructure easily and efficiently for our workloads. Rancher also allows us to comfortably scale our simulation cluster up and down and provides easy-to-deploy packages for monitoring workloads on the clusters. This makes Kubernetes a viable option for executing multi-scenario simulation experiments.

Our next step will be containerizing off-the-shelf simulation software, to provide base images of different simulation engines. This enables our research staff to develop simulation models on their office laptops and push those models to containers, that can be executed by our simulation cluster. Furthermore, we want to extend the simulation cluster as mentioned in the section that described the future architecture section.

Acknowledgements

We want to thank Uwe Langer and Alexandros Karagkasidis for their continuous hardware infrastructure support.

This research is funded by dtec.bw – Center of Digitalization and Technology Research of the Bundeswehr. dtec.bw is funded by the European Union – NextGenerationEU.

References

Anagnostou, A.; Taylor, S.J.; Abubakar, N.T.; Kiss, T.; DesLauriers, J.; Gesmier, G.; Terstyanszky, G.; Kacsuk, P.; Kovacs, J.: Towards a deadline-based simulation experimentation framework using micro-services auto-scaling approach. In: Mustafee, N.; Bae, K.-H.G.; Lazarova-Molnar, S.; Rabe, M.; Szabo, C.; Haas, P. and Son, Y.-J. (Eds.): Proceedings of the 2019 Winter Simulation Conference (WSC), National Harbor (USA), December 8th-11th December 2019, pp. 2749–2758.

Apptainer Project, 2023: Documentation | Apptainer. https://apptainer.org/docs/, accessed May 11th, 2023..

containerd, 2023: containerd overview. https://containerd.io/docs/, accessed May 12th, 2023.

Docker Inc., 2023: Docker Engine overview. https://docs.docker.com/engine/, accessed May 11th, 2023.

Hitchcock, K.: Containers. In: Linux System Administration for the 2020s: Apress, Berkeley, CA 2022, pp. 155–200.

Huawei Technologies Co., Ltd.: Container technology. In: Cloud computing technology: Springer, Singapore 2023, pp. 295–342.

Król, D.; Wrzeszcz, M.; Kryza, B.; Dutka, Ł.; Kitowski, J.: Massively scalable platform for data farming supporting heterogeneous infrastructure. In: Zimmermann, W. (Eds.): The 4th International Conference on Cloud Computing, Grids, and Virtualization, Valencia (Spain), May 27th-1st June, pp. 144–149.

Kubernetes, 2023: Windows containers in Kubernetes. https://kubernetes.io/docs/concepts/windows/intro/, accessed March 28th, 2023.

Lechler, T.; Sjarov, M.; Franke, J.: Data Farming in Production Systems - A Review on Potentials, Challenges and Exemplary Applications. Procedia CIRP 96 (2021), pp. 230–235.

MiCADO Project, 2023: Application Description Template - MiCADO. https://micado-scale.github.io/adt/, accessed April 13th, 2023.

Pappert, F.S.; Rose, O.; Suhrke, F.; Mager, J.: Simulation based approach to calculate utilization limits in opto semiconductor frontends. In: Chan, V.W.K.; D'Ambrogio, A; Zacharewicz, G; Mustafee, N.; Wainer, G. and Page, E.H. (Eds.): Proceedings of the 2017 Winter Simulation Conference (WSC), Las Vegas (USA), December 3rd-6th December 2017, pp. 3888–3898.

Podman, 2023: Getting Started with Podman | Podman. https://podman.io/docs, accessed May 11th, 2023.

Rancher Labs, 2023: Introduction | RKE 2. https://docs.rke2.io/, accessed May 5th, 2023.

Sanchez, S.M.; Sanchez, P.J.; Wan, H.: Work smarter, not harder: A tutorial on designing and conducting simulation experiments. In: Kim, S.; Feng, B.; Smith, K.; Masoud, S.; Zheng, Z.; Szabo, C. and Loper, M. (Eds.): Proceedings of the 2021 Winter Simulation Conference (WSC), Phoenix (USA), December 13th-17th December 2021, without page numbers.

Taylor, S.J.: Distributed simulation: state-of-the-art and potential for operational research. European Journal of Operational Research 273 (2019) 1, pp. 1–19.

Simulation-based Analysis of Dispatch Policies for Transportation in the Military Evacuation Chain

Martijn Braam
Department of Mechanical Engineering
Eindhoven University of Technology
Groene Loper 3, Eindhoven, 5612 AE, The Netherlands

Oliver Rose, Tobias Uhlig
Department of Computer Science
University of the Bundeswehr Munich
Werner-Heisenberg-Weg 39,
Neubiberg, 85577, Germany

Abstract

Current NATO planning relies on expert assumptions and historical data, but recent studies have shown the benefits of simulation in aiding decision-making for the military evacuation chain. In the context of a military evacuation chain, dispatch policies regarding the transportation of patients are vital. These policies encompass the placement, routing, and allocation of casualties to transporters. This paper analyses these processes in the military evacuation chain with the help of simulation. The study focuses on the earliest steps in the military evacuation chain, specifically the transportation between casualty collection points (CCPs) and the first treatment facility, in alignment with NATO's golden hour guideline. The paper narrows down the system to two CCPs and one treatment facility. The waiting times of injured soldiers at CCPs are evaluated for various dispatching policies, and insights are gained to improve the evacuation of patients. The simulation results show that a dynamic policy outperforms established static policies regarding average waiting times in certain situations where casualty arrival rates are low. The benefits of the dynamic policy decrease as arrival rates increase, but it still demonstrates better performance when there is a significant variation in arrival rates between CCPs. The findings obtained from this study may aid in enhancing decision-making within the military evacuation process and, ultimately, increase the likelihood of injured soldiers surviving.

1 Introduction

During military conflict, rapid and effective evacuation capabilities are essential to increase the survivability of casualties. Achieving this relies heavily on efficient resource allocation and proper implementation of efficient transportation policies within the military evacuation chain. The objective of the medical evacuation (MEDEVAC) system is to transfer casualties from casualty collection points (CCPs) to dedicated medical treatment facilities (NATO 2019).

To ensure proper treatment, NATO recommends the golden hour as a guideline for reaching casualties (NATO 2019). The objective of the golden hour is to provide advanced trauma care to wounded individuals within an hour of injury. This primarily concentrates on the earliest stabilization of patients and therefore this study focuses solely on the dispatching policies for the earliest steps in the military evacuation chain. The military evacuation chain is a complex logistical system with various treatment facilities and purposes. Because of this, being able to simplify the system into only the earliest evacuation logistics while focusing on the golden hour guideline can be beneficial. Analyzing this simplified system can then enhance the understanding of the complete system.

Currently, NATO uses static planning that makes several assumptions on estimated casualties and historical data (NATO 2019). Based on this, the most probable scenarios are created. Meisner et al. (2023a) and Kleint and Geck (2021) show that simulation can aid and support this planning and decisionmaking for the military evacuation chain. Frial (2022) studied the allocation of resources for evacuation using operation research. Additionally, Jenkins (2019) uses operational research to investigate the distribution of transport resources and dispatching decisions regarding aerial MEDEVAC and highlights different optimization techniques, but does not consider a simulation-based analysis.

Another study done by Jenkins, Robbins, and Lunday (2023) considers a more extensive scope of MEDEVAC optimization, including optimization of dispatch policies, by utilizing different operations research techniques. However, they do not go into great detail regarding the reallocation of resources. Due to the dynamic characteristics of combat, operation research is not sufficient for the optimization of medical planning, as stated by Yue, Marla, and Krishnan (2012). This incentivizes a simulation-based study on the performance of dispatching policies for evacuation. Meisner et al. (2023b) pointed out that constructive simulation is essential for verifying medical plans and that current models lack the flexibility needed to represent the dynamics of combat. This is especially needed for testing new medical dispatching policies. To evaluate current and future concepts, they propose a constructive simulation where the military evacuation chain is studied.

This paper closely aligns with the research conducted by Meisner et al. (2023a) to aid the planning and decision-making of the military evacuation chain with the help of simulations. The authors propose a modular simulation concept that is flexible and capable of efficiently implementing new decision rules or concrete strategies. The focus of this paper is on analyzing different dispatch policies for ground-based vehicles. In particular, static dispatch policies are compared to a dynamic one, by modeling and simulating a sub-part of the military evacuation chain. This sub-part evaluation of effectiveness is conducted because the modeling process of the dynamic dispatch is time-consuming. This can then be further implemented in a full-scale simulation as proposed by Meisner et al. (2023b).

The subsequent sections of this paper will first start with the description of the case study. This chapter provides details about the problem description, system analysis, an analysis of the different dispatch policies, and simulation input. Second, the results are presented, which is followed by the discussion, which informs about the analysis of the results and describes the limitations of the study. Finally, the conclusion is presented which which summarises the study and delves deeper into potential further research.

2 Case Study

This chapter describes the case study that is conducted for this paper. The problem description, system analysis, dispatch policies, and simulation input are described here.

2.1 Problem description

Due to the limited resources that are available in the military evacuation chain, proper allocation of transportation vehicles can benefit the survivability of casualties.In practice, transportation vehicles are assigned to specific CCPs, sometimes even to multiple ones, or to a designated treatment area. (NATO 2018). The trucks drive back and forth between CCPs and treatment areas to stabilize injured soldiers as soon as possible. Dispatch policies that are used to determine the allocation of transportation vehicles are analyzed to see the impact of the average waiting time of casualties. A model is created to demonstrate the effect of these dispatch policies. Specifically, static dispatch policies are compared to a more dynamic policy. By comparing different policies, insight can be gained into the average waiting times of injured soldiers at the CCPs. This can result in an improved allocation of dispatch policies by medical planning personnel.

2.2 System analysis

The military evacuation chain starts with the arrival of casualties at certain casualty collection points, after which they get transported to four different roles (NATO 2019). These roles are treatment areas that contain certain medical facilities with different capabilities. Role 1 acts as a treatment facility that can. provide primary health care, triage, and can stabilize casualties while Role 2 can also provide surgical interventions. Additionally, Role 3 and Role 4 extend Role 2 capabilities by providing similar functions as civilian hospitals (Hodick`y, Procházka,

Jersák, Stodola, and Drozd 2020). Based on the severity of the soldiers' wound or condition, roles can be skipped. In practice, numerous casualty collection points exist in the system that need to be considered, in addition various roles. This can make an analysis of the complete logistical system complex.

The transportation between the casualty collection points and the first treatment facility is of great importance due to NATO's golden hour guideline, where MEDEVAC and advanced trauma care assets must be capable of reaching the casualty within one hour of wounding. Because of the importance of the transportation between the CCPs and the first treatment facility, we simplified the system to only consider this part of the military evacuation chain. We consider a system that consists of two CCPs and one treatment area (Role 1). In between these points, soldiers get transported. Figure 1 displays this 3-node construction.

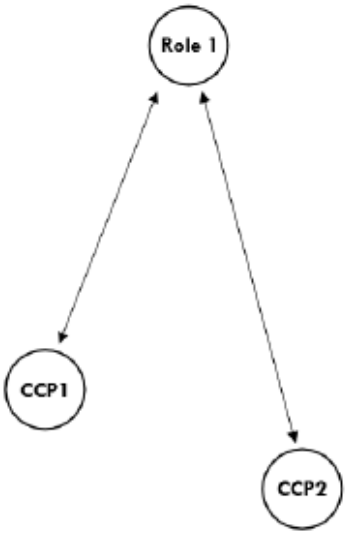


Figure 1: 3-node evacuation system

To assess the system's efficiency, we categorize injured soldiers into three tiers based on their injury. Based on that, we assign maximum waiting times that the soldiers are allowed to wait at a CCP until treatment is required. These tiers reference the triage categories that NATO considers (NATO 2019). Here Tier 1, Tier 2, and Tier 3 are characterized by life-threatening injuries, severe but not life-threatening, or minor injuries, respectively. We assign maximum waiting for these tiers as one hour for Tier 1, 24 hours for Tier 2, and one week for Tier 3. Tier 3 casualties can be considered as being able to care for themselves. Therefore, a maximum waiting time of 1 week is assigned, and the golden hour rule is relaxed. Since Tier 2 patients are severely injured but are not in an immediate life-threatening condition, the maximum waiting time that is considered for this patient is 24 hours. Because Tier 1 patients have life-threatening injuries, we assume treatment later than 1 hour will be lethal. It is important to note that these waiting times are not from any NATO guidelines but are used as estimates to decease. Based on these maximum waiting times, the soldiers are prioritized so that the injured soldiers with the most urgent need of treatment, get evacuated and therefore treated first.

Figure 2 displays the evacuation process of a casualty on a conceptual level. The process starts when casualties arrive at a specific CCP. When one arrives, a casualty is assigned a tier based on its injuries. This determines the maximum allowed waiting time at a CCP. When this time exceeds, we assume the casualty has died, and therefore, this waiting time is used as to prioritize the casualty. Additionally, a determination process starts to see if a truck request is necessary. The determination process looks at the number of casualties at the CCP and the vehicles already going to this CCP. Then, it assesses whether there is still enough capacity for the newly arrived casualty, or a new transport vehicle is needed. If so, no further actions are required and the casualty is assigned to an already requested vehicle for evacuation. If the capacity of the already requested vehicles is not enough, and there are still vehicles idle, a vehicle is requested. As soon as a medical vehicle arrives at the CCP, it will load up as many casualties as it can handle and will drive back to Role 1, where medical services can be facilitated to the patients. As soon as a vehicle arrives at Role 1 and has delivered all soldiers, it will assess if any casualties at a CCP are not allocated to a vehicle yet. If this is the case, the vehicle will drive towards this casualty. In the case that casualties at both CCPs require transport, the transportation vehicle will drive towards the casualty with the highest priority.

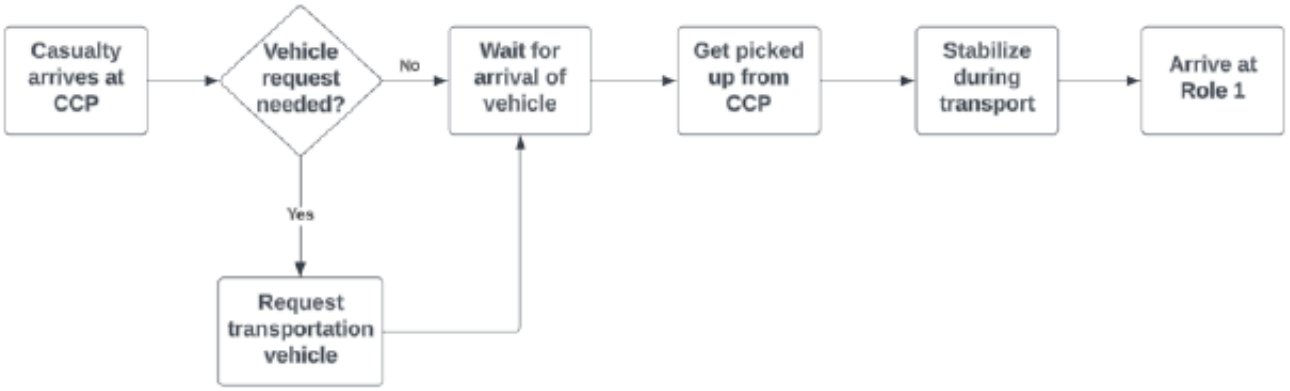


Figure 2: Process of casualties getting evacuated

2.3 Dispatch policies

Three different dispatch policies are modeled. All three policies are visualised in 3 and are explained in the next section.

2.3.1 Policy A [Static]

In this policy, the transportation vehicle is located at the CCP, as shown in Figure 3a. With this policy, the vehicle will always return to its designated CCP when idle. This has the advantage of immediately transporting the first soldier that arrives at the CCP. A more practical advantage is the fact that no communication is required between the CCP and the treatment area. The requested transportation vehicle will already be at the CCP, or drive back to the CCP after dropping off patients. However, with this policy, the transportation vehicles will be allocated equally over specific CCPs. This means one transportation vehicle can only transport patients from their designated CCP. If the arrival rates at the CCPs differ significantly, it may be preferable to allocate resources differently among the CCPs to optimize resource allocation. An additional disadvantage is the fact that transporters and medical staff located at the CCPs will be closer to the combat area.

Since transportation vehicles will always go to the destination they are initially assigned to, this policy is determined as a static policy.

2.3.2 Policy B [Static]

In this model, the transportation vehicles are located at Role 1 as shown in Figure 3b, and will also stay at Role 1 when idle. Additionally, the transportation vehicles are not pre-assigned to a specific CCP, meaning all trucks are allowed to go to all CCPs. One advantage of this approach is that it can lead to more efficient allocation of resources when CCP arrival rates vary, since the vehicles are not strictly allocated to a specific CCP. A disadvantage, however, is the fact that each vehicle has to drive towards a CCP after casualties arrive, resulting in longer waiting times that depend on the travel time if the vehicle wasn't already on its way to the CCP. This is not the case with Policy A, because then idle vehicles will stay at the CCP.

We define this policy as a static policy, because after a CCP is allocated to the vehicle, it cannot switch directions and change its destination.

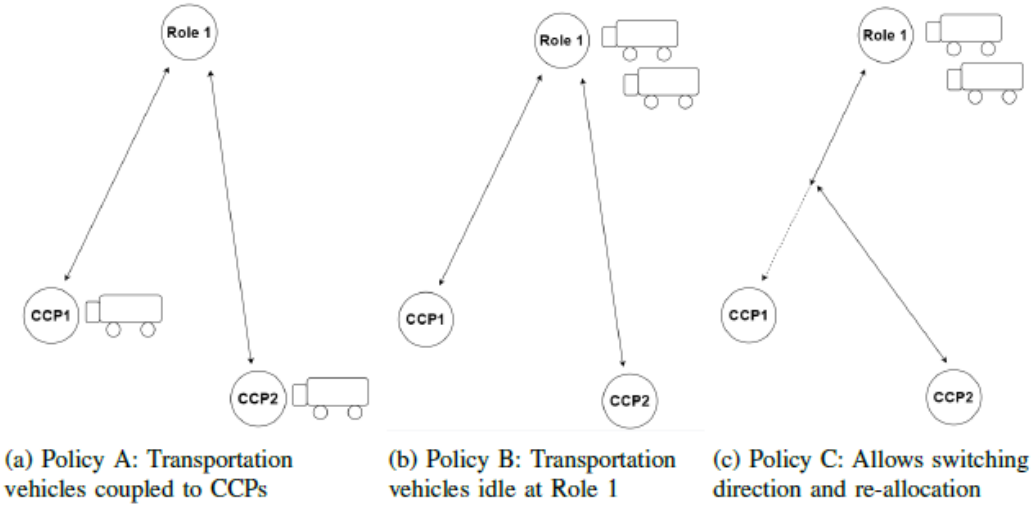
2.3.3 Policy C [Dynamic]

This model also keeps the transportation vehicles at Role 1 when idle, as shown in Figure 3c. However, with this policy, transportation vehicles are allowed to switch their destination while driving. This means that when a truck is driving to a CCP, but a casualty with a higher priority arrives at a different CCP, this vehicle can switch its route. This policy wants to emphasize that, on average, the soldiers with the least amount of allowed waiting time will also have the least amount of waiting time. Additionally, transportation vehicles are able to drive back to any CCP after they have already picked up soldiers as long as there is still capacity for this. For this, a threshold in distance is

implemented in the model to avoid reassigning the vehicle when it is close to its destination.

With this policy, a transporter can pick up soldiers of CCP1 as well as CCP2 before dropping them off at Role 1. It is, however, important to note that there is no planning involved. When a transporter has picked up soldiers, it drives back to Role 1. If soldiers arrive at both CCP1 and CCP2, two different vehicles is sent to CCP1 and CCP2. Even if sending one vehicle to CCP1 and letting it afterwards drive to CCP2 would be more beneficial from a holistic point of view.

We call this policy a dynamic policy because the reallocation of vehicles can occur after the initial allocation of CCPs.



(a) Policy A: Transportation vehicles coupled to CCPs

(b) Policy B: Transportation vehicles idle at Role 1

(c) Policy C: Allows switching direction and re-allocation

Figure 3: Visualization of the three policies

2.4 Simulation input

Discrete event simulations have been conducted in AnyLogic to analyze the different average waiting times of the casualties that arrive at the two CCPs. Table 1 displays the input data for the model that is kept fixed for all conducted simulations, while varying the average arrival rates of casualties.

Simulation duration	50 days
Number of transportation vehicles	2
Vehicle capacity	8 casualties
Vehicle speed	30 km/hour
Re-allocation threshold distance	1km
Average distance between RS and CCP	14.77km
Tier 1 time till treatment	1 hour
Tier 2 time till treatment	24 hours
Tier 3 time till treatment	1440 hours
Tier 1 occurrence	22%
Tier 2 occurrence	23%
Tier 3 occurrence	55%

Table 1: input data used for all simulations

The number of available vehicles is set to the number of CCPs and the vehicles are capable of carrying eight casualties and drive 30 km/h. The different tiers that are allocated to the casualties depend on their injuries. The occurrence rate of this is not publicly available, but is realistic according to experts. The location of both CCPs and Role 1 is fixed. The average distance between the CCPs and Role 1 is in this case 14.77km. This determines, together with the vehicle speed, the duration of evacuating casualties. Also,. the threshold in switching directions of the vehicle is set at 1km, meaning when a vehicle is within 1km of its destination, it will always continue its path and ignore the arrival of higher priority casualties. This only applies to the application of Policy C. We assume an exponential arrival rate with varying averages, as will be explained later.

Further assumptions include that each transportation vehicle is equipped with medical equipment and is capable of stabilizing the patients in the vehicle. Therefore, it can be assumed that the time till

treatment stops as soon as a casualty enters the transportation vehicle. Also, while communication in practical instances will not be instant and always available, it is presumed to be so for the purpose of this case study. Breakdowns and downtime of resources are also neglected for this study. Additionally, it is assumed that transportation vehicles have complete freedom in transportation direction without being constrained by roads, traffic, or geographical limitations. Furthermore, it is assumed that Role 1 always has the capacity to treat all patients and, therefore, does not constrain the dispatch policy.

3 Results

This section describes the results of simulating different dispatch policies. Different simulation runs have been conducted to assess these dispatch policies. Each individual simulation gave insight into the average waiting time of each of the tiers with given inter-arrival rates. This can then be compared to the simulation with the same arrival rates but with different policies. Before running the simulation, the limits of the system are estimated. This is possible for Policy A and B because of their fixed traveling distance. As mentioned in section 2, the average distance between the CCPs and Role 1 is 14.77 km. The transportation vehicle will, therefore, travel almost 30km for the evacuation of a maximum of 8 patients, resulting in a maximum capable arrival rate of 16 casualties per CCP per transportation vehicle. This information is used as a reference for changing the average arrival rates of the casualties.

In Figure 4, the average waiting times are displayed for the three different policies, where casualties are differentiated by the three different tiers. The different colors display the different casualty tiers, which are grouped per policy. With an average arrival rate of four casualties per hour per CCP, there is barely any difference in waiting times between policies A and B. However, Policy C where switching can occur, is significantly better performing, especially for the Tier 1 soldiers. Furthermore, we see that as the arrival rates of soldiers increase, the benefits of the switching policy decrease with respect to policies A and B as long as the ratio between arrival rates of CCPs stays equal. This can be seen when comparing Figures 4, 5, and 6.

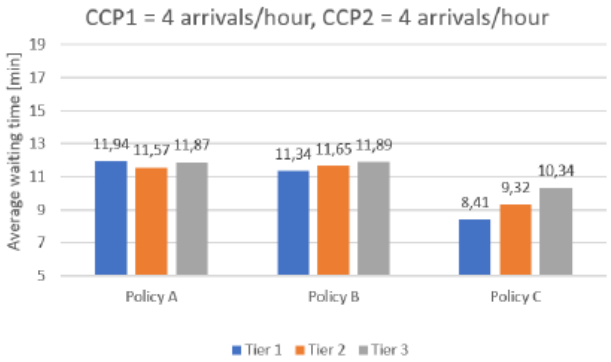


Figure 4: Average waiting time of casualties with arrival rate of 4 per hour at CCP1 and CCP2

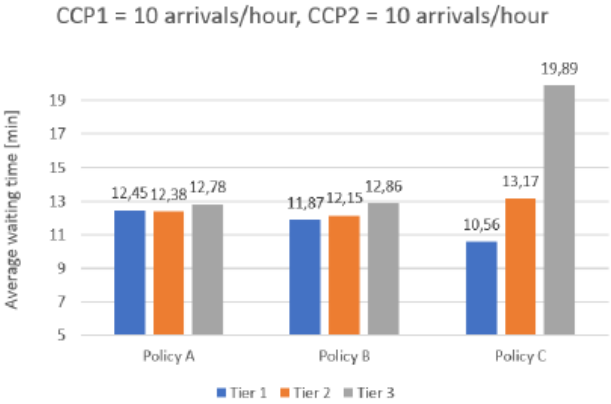


Figure 5: Average waiting time of casualties with arrival rate of 10 per hour at CCP1 and CCP2

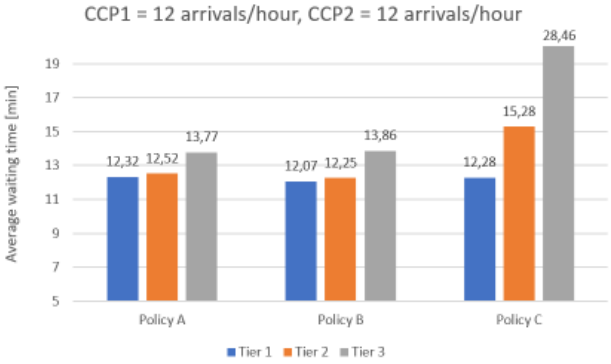


Figure 6: Average waiting time of casualties with arrival rate of 12 per hour at CCP1 and CCP2

Figure 7 and Figure 8 display the average waiting time for scenarios where there is a high variety in arrival rates between the CCPs. In Figure 7, it is clear to see that Policy B is beneficial with respect to Policy A due to the lower average waiting times. Even better

performance is achieved by Policy C, where average waiting times go down to below 8 minutes for Tier 1 casualties. What can be noticed from Figure 8, is the lack of waiting times of Policy A. This has to do with Policy A having over-capacity, due to the fact that one transportation vehicle can transport up to 16 casualties per hour and Policy A cannot utilize multiple vehicles for one CCP.

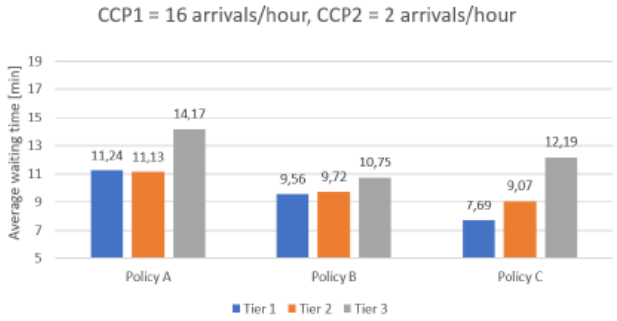


Figure 7: Average waiting time of casualties with arrival rate of 16 per hour at CCP1 and 2 per hour at CCP2

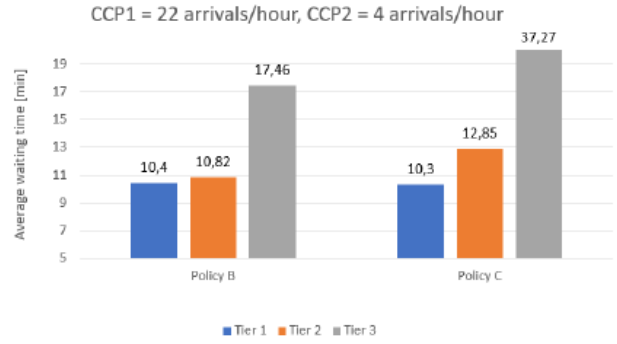


Figure 8: Average waiting time of casualties with arrival rate of 22 per hour at CCP1 and 4 per hour at CCP2

Policy A cannot allocate two vehicles to one CCP. Because of this, Policy A fails to evacuate casualties at CCP1, where 22 casualties arrive per hour, whereas Policy B can potentially handle up to 32 arrivals per hour in total. Determining the limit of casualty arrival rates for Policy C is less trivial since the traveling distance is not fixed. When reallocating the transportation truck from one CCP to another, it will drive additional kilometers, depending on the timing of reallocation. Travel distance is also increased when the vehicle gets reallocated to a CCP after it already picked up casualties.

Figure 9 shows the average kilometers that have been driven as a bar chart per simulation for Policy C. In this figure, the numbers below the bars display the arrival rates. E.g., "16,2" refers to 16 arrivals per hour at CCP1 and two arrivals per hour at CCP2. Additionally, the increased number of total casualties for the 50 days simulations are displayed, with reaching 30.000 casualties at maximum. Policy C does see anaverage decline in kilometers driven per evacuation from 27km to less than 20km. This is, however, still more than the fixed 14.77 km that are driven for an evacuation for policies A and B.

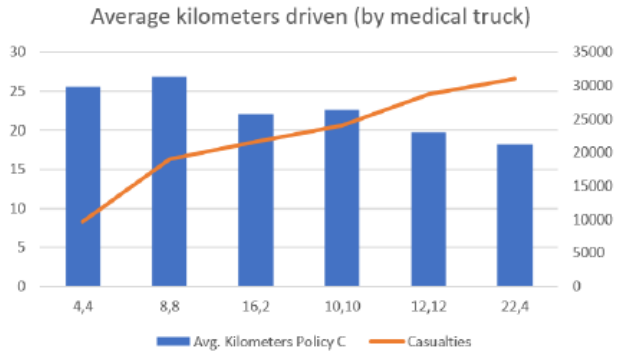


Figure 9: Average kilometers driven by medical trucks per simulation of Policy C

4 Discussion

This simulation study reveals that average waiting times for different tiers of casualties vary, depending on the policy. With relatively low arrival rates we see a benefit of Policy C, where switching directions and re-entering to CCPs is possible. The average waiting time of Tier 1 soldiers is then significantly improved. However, as the arrival rate increases, the positive effects of Policy C start to diminish and can even get slightly worse at a certain threshold. This is likely due to the fact that, with the use of a switching policy, transportation vehicles are driving more kilometers before dropping off patients compared to the policies where the vehicles will drive in a straight direction. While this characteristic can help in the quick evacuation of varying prioritized casualties, it lowers the utilization of the resource as soon as arrival rates increase. Additionally, the waiting times of Tier 2 and Tier 3 soldiers are getting longer, compared to the other policies. This is likely because of the focus on prioritization of Tier 1 casualties. While waiting times for Tier 2 and Tier 3 casualties increase because of this,

it can be seen as less critical since the allowed maximum waiting times are a lot higher.

When a wide variety of arrival rates occurs between different CCPs, we also note differences. When the arrival rates are equal, barely any difference can be noted between Policy A and B. However, when the arrival rates differ, we see an improved result in average waiting times for Policy B. Here, the transportation vehicles are stationed at Role 1 and can be requested by either CCP, where the waiting times are shorter due to improved resource allocation. At an arrival rate of more than 16 soldiers per hour, we note over-capacity of Policy A, showing that Policy A can only be used with lower arrival rates due to the dedicated allocation of vehicles to CCPs.

Again, Policy C shows an increase in performance with lower arrival rates, especially when arrival rates vary between CCPs. Because reallocation of the transportation vehicles is utilized, a vehicle that is on its way to a CCP with low arrival rates, can switch its destination when necessary, which improves performance.

Although the primary focus of this research paper is the transportation process of soldiers to a treatment area, it is important to recognize that the case study's findings and methodologies can have broader implications. The principles and decision policies explored in this study can be extrapolated and applied to various domains such as logistics, manufacturing, or supply chain management. By examining the challenges posed by limited resources and a variety of exponential arrival rates of soldiers, valuable insights can be gained into enhancing decision-making processes in different fields.

It is important to acknowledge the limitations of this research. This analysis has only been done for the situation where two CCPs and one treatment facility have been considered. The location of these points with respect to each other might highly affect the efficiency of each policy. Additionally, communication capabilities have been considered to be constantly available, which is unrealistic in a combat scenario. Greater insight can also be gained by exploring the utilization of the transportation vehicles in more detail, and comparing this for each policy.

5 Conclusion

This paper focuses on the analysis of static and dynamic dispatch policies in the military evacuation chain, specifically regarding the transportation of injured soldiers. By using discrete event simulations, this study aims to explore different dispatch policies and evaluate their impact on average waiting times for casualties. The results of the study demonstrate the effectiveness in different situations. Three dispatch policies have been examined, each employing different transportation heuristics.

Based on the simulation results, it is evident that a transportation vehicle that changes direction according to casualty priority is beneficial in decreasing waiting times, particularly during periods of low arrivals. However, this advantage decreases as the arrival rates increase. This is due to the increased distance

traveled, where it becomes more advantageous to drive toward CCPs without changing directions. The same is true when there is a significant variation in arrival rates between two CCPs.

The findings of this study contribute to enhancing decision-making processes within the military evacuation chain. By identifying the most effective dispatch policy, medical planners can make informed decisions to allocate resources and prioritize the transportation of injured soldiers. The reduction in waiting times can have a significant impact on the chances of survival and overall outcomes in military combat scenarios. The findings demonstrated the effectiveness of different policies in reducing waiting times for casualties, with Policy C showing improved performance with low and varying arrival rates over the CCPs. For scenarios where arrival rates are greater and approach the limitations of the system, policies A and B show improved performance. This highlights the importance of considering dynamic routing strategies to optimize transportation efficiency in the military evacuation chain.

Future research can build upon the findings of this study by exploring additional policies and increasing complexity by adding additional treatment facilities and CCPs. Since this study shows the benefits of different policies in different situations, considering an overall dynamic policy of switching between policies based on the arrival characteristics of casualties, can be beneficial to optimize the military evacuation chain.

References

Frial, V. B. 2022. "Evaluating the Military Medical Evacuation Dispatching and Delivery Problem via Simulation and Self-Exciting Hawkes Process".

Hodickỳ, J., D. Procházka, R. Jersák, P. Stodola, and J. Drozd. 2020. "Optimization of the casualties' treatment process: blended military experiment". *Entropy*.

Jenkins, P. R. 2019. "Strategic location and dispatch management of assets in a military medical evacuation enterprise".

Jenkins, P. R., M. J. Robbins, and B. J. Lunday. 2023. "Optimising aerial military medical evacuation dispatching decisions via operations research techniques". *BMJ Mil Health*.

Kleint, R. and Geck, A. 2021. "Simulation-Based Decision Support for the Logistic System of the German Armed Forces". //www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-184/MP-MSG-184-13P.pdf, accessed 24.10.2023.

Meisner et al., K. 2023a. "Konzeptionierung eines Simulationsmodells der Rettungskette unter Gefechtsbedingungen". *Simulation in Produktion und Logistik 2023*.

Meisner et al., K. 2023b. "A modular simulation model for mass casualty incidents".

NATO 2018. "Allied Joint Medical Doctrine for Medical Evacuation".

NATO 2019. "NATO standard AJP-4.10: allied joint doctrine for medical support edition C version 1 with UK elements". *Ministry of Defence*.

Yue, Y., L. Marla, and R. Krishnan. 2012. "An efficient simulation-based approach to ambulance fleet allocation and dynamic redeployment". In *Proceedings of the AAAI Conference on Artificial Intelligence*.

6G Technology Ecosystem Vision: a Dual Use Approach in Defence and Sovereignty of Countries

Giovanni Gasbarrone
https://www.linkedin.com/in/giovanni-gasbarrone-7b7244/
Vice President ANUTEI
http://www.anutei.it/

Abstract

Digital technologies are also becoming a fundamental and essential means of ensuring the sovereignty of countries. The development of European-based 6G infrastructure and solutions is one of the keys to ensuring European sovereignty in critical technologies and systems in all vertical sectors and in military industries .

For this strategic and vital objective for the survival of the industry, the EU has launched a first research program of 240 million euros for 6G, thus hoping to maintain technological sovereignty after 5G also in 6G references: (World Economic Forum, EU, and Advisory board : IOTHINGS World)

Next generation 6G and "Quantum Technologies represent a revolution in military operations that will change in the future the way of operations, from cybersecurity to communications in tactics, operational and warfare strategies in modelling & simulation. Quantum technologies are dual-use technologies, and therefore are of interest to the defence and cyber security industry and military.

The recent RADAR systems and the 5G and 6G antennas have contiguous or even overlapping operating principles that allow the development of solutions in a dual use perspective.

The convergence between radar and telecommunications can be glimpsed in the use of electronically scanned antennas that for 5G and 6G transmissions use "smart antennas" MIMO - Multiple Input Multiple Output. In the future, we begin to glimpse the evolution towards quantum radar while the "quantum" revolution in 6G with cognitive radio will be the next generation architecture thanks to quantum computers that already allow in 5G the optimal cellular planning of frequencies and transmission network. We are now working on the fusion of technologies with Quantum Machine Learning for 6G networks.

A fundamental role in this new scenario is the "hyper connectivity" beyond 5G to enable quantum computers and quantum communications. Today, European critical infrastructures and public safety communications and cloud are vulnerable to cyber-attacks Today advances in supercomputing and the advent of quantum computing may soon undermine modern encryption systems, threatening the security of transmitted data and secure access to remotely cloud infrastructure.

1 Quantum computing in 6G and Artificial Intelligence

Quantum Computing will support the development of innovative services, and one of the new areas of research and innovation in industry is the synergy of quantum computer with artificial intelligence (AI). The AI domain is a reality and therefore many applications will be deployed with AI to support next-generation wireless communications. It is no doubt : one of the industries that profit most from artificial intelligence technologies is that of wireless communications, as AI is incorporated into both smartphones and cellular architecture to control services and network resources. The 6G network will manage billions of devices, thanks to quantum computing and artificial intelligence platforms. Digital technologies are also becoming a fundamental and essential means of guaranteeing the sovereignty of countries. The development of 6G infrastructure and solutions based in Europe is one of the keys to ensuring European sovereignty in critical technologies and systems.

Today about 40% of tecnolgies in 6G (IPR, chipsets) are under the full property of China : this means that China accounts for 40% of 6G patent ICT applications.

For this strategic and vital goal for the survival of the Industry, the EU has launched a first research program of 240 million euros for 6G, thus hoping to maintain technological sovereignty after 5G also in 6G.

The new "Next generation" 6G communication systems are already born intelligent, and will provide the major industry sectors with a platform that will allow them to make the best use of the scarce resource of the spectrum thanks to an ethergeneous network architecture that requires cognitive radio to be realized.

The next decade will see 6G connect billions of device entities, sensors and connected vehicles, in a scenario where robots and drones will generate Zettabytes of digital information. 6G will improve 5G applications with more stringent requirements, such as holographic telepresence and immersive communication, and meet even stricter parameters than 5G.

Starting from 2030, we could see the advent of the era in which the use of personal mobile robotics will interact with next-generation Artificial Intelligence platforms thanks to neuronal systems offered by the connectivity of the 6G network.

6G is the generation of mobile networks that will help us to face the socio-economic challenges in which the way of living and working will make a new paradigm shift compared to 5G.

6G will be an autonomous ecosystem based on artificial intelligence. 6G will offer complete wireless connectivity almost instantaneous and without restrictions thanks to the cognitive radio in which artificial intelligence falls both in the mobile device and in the management of radio interfaces.

Artificial intelligence will be both local and distributed thanks to fog computing architectures and quantum computing capabilities. "AI everywhere" is the mantra of the new network.

6G is the generation of mobile networks that will help us face these socio-economic challenges in which the way we live and work will make a new paradigm shift. It will progressively evolve from being human-centric as in 5G, to being both human and machine-centric.

6G will offer almost instantaneous and unrestricted full wireless connectivity thanks to cognitive radio in which artificial intelligence is integrated into both the device and the management of the radio interfaces.

2 Towards 6G

Among the innovative wireless technologies, those of Software Defined Radio and Cognitive Radio will be able to adapt to changes in the environment, interference and availability of licensed and unlicensed frequencies, thus contributing to traffic management in communications between different systems, even in operational scenarios that include more flexible spectrum management methodologies.

Cognitive Radio is an intelligent technology in dual use approach, that explores the spectrum by exploiting gaps in unlicensed or underused frequencies and their spatial availability. In the 6G communication network, devices such as smartphones interact with the base radio stations of the cellular network and receive indications in which spectrum they can find more favorable conditions in terms of greater availability for frequencies and bit rates. This technology will be available on .a dual use approach.

However, this technology, capable of guaranteeing dynamic and no longer static access to the radio spectrum, presents some complexities for its implementation, linked in particular to the aspects of legislation and regulation of access to frequencies. These new technologies offer a series of potentialities and advantages because they make it possible to optimize radio resources and investments and thus obtain efficient planning in the use of fixed and mobile networks, offering global mobility to users in a framework in which security is always at the heart of the design requirements. The 6G architecture is based on quantum computing, hyperconnectivity and new radio technologies (fig 1).

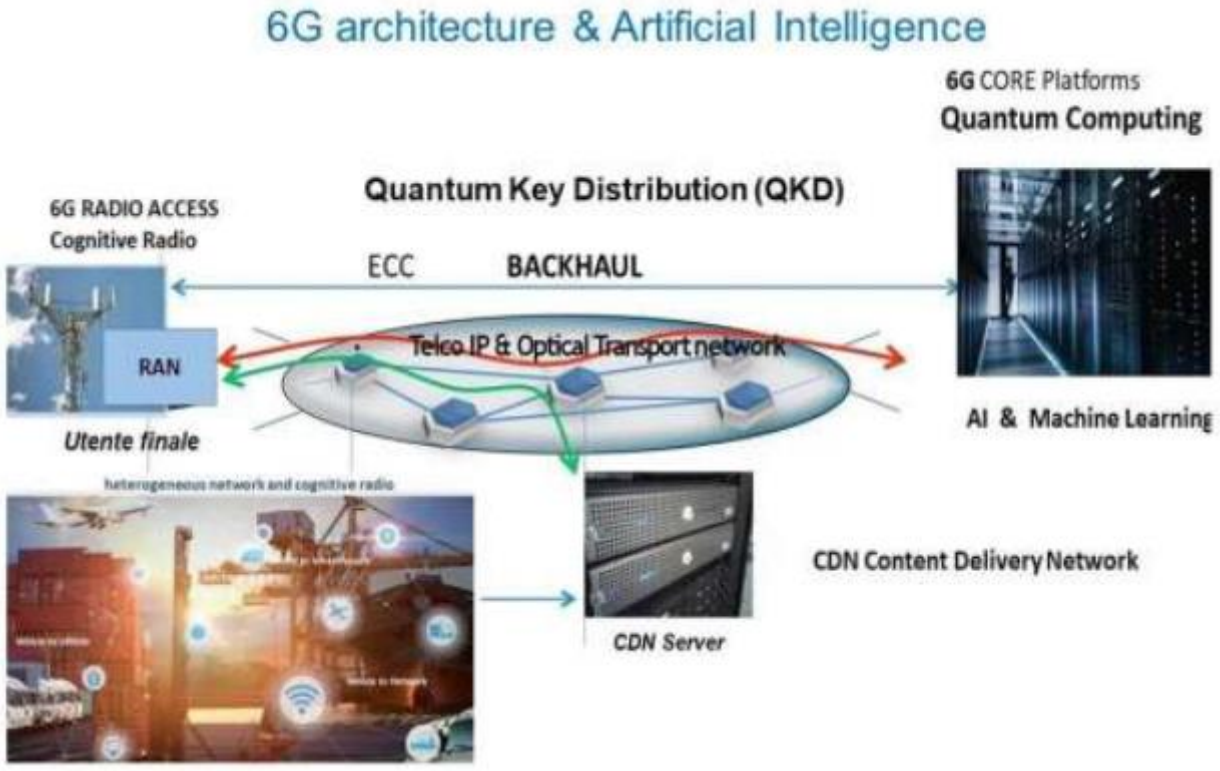


Fig 1: 6G network architecture is based on Artificial Intelligence, new radio interface and quantum computing

Digital technologies like IOT and towards 6G are becoming even a fundamental and essential means of guaranteeing the sovereignty of Europe.

The development of 6G infrastructure and solutions based in Europe is one of the initiatives. at EU level to ensure the future and European sovereignty in critical technologies and systems. In the immediate future, the 5G class of Ultra-Reliable Low-Latency Communications, it is particularly indispensable in real time and mission critical applications. High reliability is required in many "Industrial IoT" applications that have stringent requirements for cybersecurity, such as smart grids in energy, and robotics.

Interview with Giovanni Gasbarrone member of the IOTHINGS WORLD Advisrory Group :

"Digital transformation and IoT are key values in modern industry: a dual use approach".

Today there is more and more talk of Industrial IoT which in 5G finds a system of connectivity and reliability and low latency. These are solutions that are ultra reliable for mission critical situations in augmented reality (fig.2) . It is Giovanni Gasbarrone, Advisory Group IOTHINGS, who illustrates this and

other considerations during the Roman event of Iothings World. Waiting to see and listen to him in Milan, during the two days, next 11 and 12 October, Gasbarrone even speaks of an acceleration towards a concept of Industry 5.0 moving towards 6G, aiming towards 2030 with a consensus of low latency and low power consumption. All you have to do is watch and listen to the interview

https://www.thenextfactory.it/2023/05/gasbarrone-lindustria-moderna-vuole-iot-e-digitaltransformation/

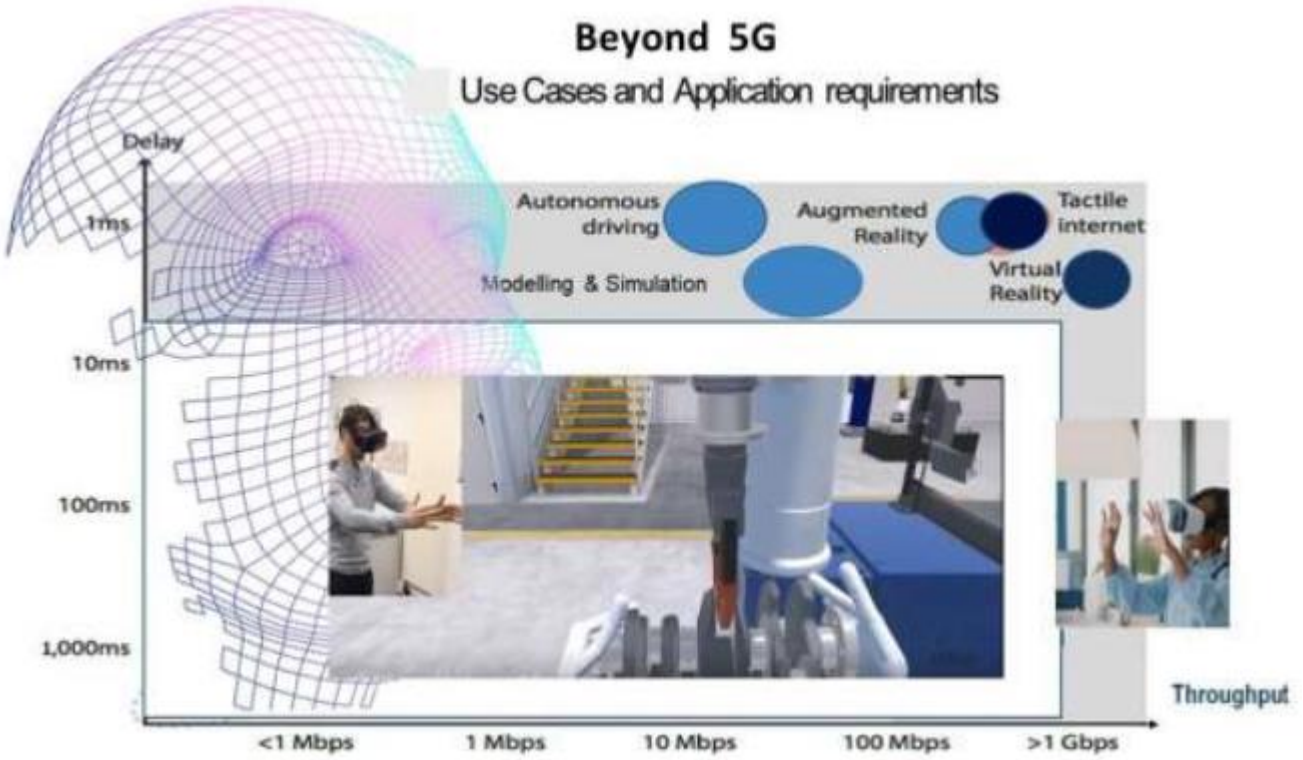


Fig 2: Beyond 5G: use cases and application requirements in Modelling & Simulation dual use applications

It will be possible to make holographic calls on the 5G both satellire and terrestrial/maritime networks and thanks to the viewers available for virtual and augmented reality with 5G smartphones it will be possible to participate in 3D battlefield simulation and real time by sharing them from commad & control tablets. Augmented reality and virtual reality are the applications that will travel on the 5G network thanks to the increased bandwidth: a real killerapplication.

The next dual use cases, therefore, see the interaction with holograms in the battle field operations command & control in which the evolution of augmented reality takes place with 5G thanks to its very low latency and very high bandwidth characteristics through the creation of a space for virtual battlefield. in which the organizer's avatar interacts with those of colleagues who are in other locations, sharing multimedia content in the 3D work tables (fig 3)

2.1 Towards 6G: models and strategies for the Italian and EU ecosystem

In the international scenario of global competition, with a first mover strategy in April 2022, the President of the United States, Joe Biden, and the Japanese Prime Minister, Yoshihide Suga, signed an agreement for a joint investment of 4.5 billion dollars for R&D in 6G networks.

Korea is engaged together with Taiwan's microchip manufacturers in researching new technologies for

the development of 6G. China, which currently holds the supremacy in patents, is surrounding Taiwan because it is aware that it will be at the center of the development of 6G for components: micro-antennas, sensors and new-generation microchips that will have to be produced in unimaginable quantities.

The US Department of Defense's dual use approach described in the press release on "beyond 5G and 6G research programs" fits into this scenario:

"Three New Projects for DOD's Innovate Beyond 5G Program "

Aug. 2, 2022 | Public Release

https://www.defense.gov/News/Releases/Release/Article/3114220/three-new-projects-for-dodsinnovatebeyond-5g-program/

The Department of Defense's Innovate Beyond 5G (IB5G) Program recently kicked off three new projects that continue to advance DoD collaborative partnerships with industry and academia for 5G-to-NextG wireless technologies. "The DoD has a vital interest in advancing 5G-to-NextG wireless technologies and concept demonstrations," said Dr. Sumit Roy, IB5G Program Director. "These efforts represent our continuing investments via public and private sector collaboration on research & development for critical Beyond 5G technology enablers necessary to realize high performance, secure, and resilient network operations for the future warfighter."

Open6G is a new industry-university cooperative effort that aims to jumpstart 6G systems research on open radio access networks (Open RAN). The effort will focus on Open RAN research and open source implementation of 5G protocol stack features to support emerging beyond/enhanced 5G applications. Open6G will serve as the DoD's hub for development, testing, and integration of trusted enhancements, supporting an industry and federal government NextG ecosystem pursuing 6G technology goals."

2.2 Beyond 5G : 6G and quantum computing - an european strategy

The 6G network will manage billions of devices, thanks to quantum computing and artificial intelligence platforms. Digital technologies are also becoming a fundamental and essential means of guaranteeing the sovereignty of countries. The development of 6G infrastructure and solutions based in Europe is one of the keys to ensuring European sovereignty in critical technologies and systems.

For this strategic and vital goal for the survival of the Industry, the EU has launched a first research program of 240 million euros for 6G, thus hoping to maintain technological sovereignty after 5G also in 6G.

Economics fundamental in 6G and microelectronis are essential means of ensuring the sovereignty of countries.
The development of European-based 6G infrastructure and solutions is one of the keys to ensuring European
sovereignty in critical technologies and systems EU accounts for just 4% of a €400 billion telecommunications equipment market excessive supply chain dependency at the expense of sovereignty/security aspects

• New communication architecture (Open RAN) that challenges consolidated positions
• New opportunities for device connectivity beyond smartphones
• New radio systems planned, new applications, JCAS
• High influence of the chipset industry on standards (5G NR,…), and where most of the industry resides (USA)
• Chipset Industry Makes Money on 5G Investments!

it is Crucial to bring the microelectronics industry in the early stages of R&D, such as in the US, China, Korea, complete value chain approach.

2.3 Micro Electronics and 6G in Europe : which strategies and economics

o Chips Act: EU accounts for just 4% of a €400 billion telecommunications equipment market

o Excessive supply chain dependency at the expense of sovereignty/security aspects

o New communication architecture (Open RAN) that challenges consolidated positions

o New opportunities for device connectivity beyond smartphones o New radio systems planned, new applications, JCAS

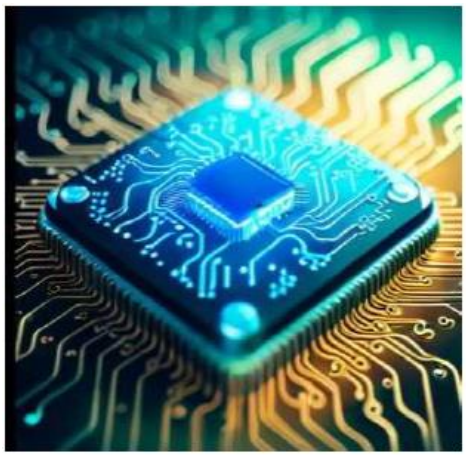
o High influence of the chipset industry on standards (5G NR), and where most of the industry resides (USA)

o Chipset Industry Makes Money on 5G capex

o it is Crucial to bring microelectronics industry into early stages of R&D, such as in US, CN, RoK, complete value chain approach

3 Microchip markets expected to grow 9% through 2030

5G & &6G data driven network chipset market is booming



3.1 Artificial Intelligence and machine learning chipsets market

Market outlook will be 15% by 2025 of Total chipset market value about 800 €bn

The 5G & 6G and any other future wireless networks and Devices will be designed on Artificial Intelligence chipsets accross all architecture domains : Edge, Core, access

6G Outlook EU Context

https://digital-strategy.ec.europa.eu/en/library/6goutlook

In the last TTC2 conclusions the European Union and the United States recognised "the importance of emerging technologies for global prosperity and security" and stated that they "are committed to exchange information and explore opportunities for collaboration in our research and development agendas, notably for Artificial Intelligence ("AI"), telecommunication technologies beyond 5G and 6G, and quantum computing. Given that 6G will be a critical global infrastructure, common approaches towards 6G international standards are particularly relevant."

3.2 The EU response to the semiconductor crisis: the Chips Act

The EU Chips Act is the microchip industry defense action due to the global competition for the control of digital technologies . High tech industry forces European companies, public administration and research centers to interact and use the information technologies they need such as microchips and artificial intelligence even outside the European Union. National protectionism is also a weapon that Europe and Italy are using with the golden power against the acquisition

3.3 6G and Quantum network infrastructure : an european strategy

Europe is the major leader in terms of fundamental research and public support. However it faces a strong competition and is under pressure for industrial merger & acquistion process from chinese state owned companies.

The EuroQCI initiative aims to build a secure quantum communication infrastructure that will span the whole EU, including its overseas territories.

The participating countries are working with the European Commission and the European Space Agency (ESA) to design, develop and deploy the EuroQCI. The aim is for it to be fully operational by 2027.

The European Quantum Communication Infrastructure (EuroQCI) Initiative | Shaping Europe's digital future (europa.eu)

https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

3.4 Towards an operational EuroQCI

Work on the EuroQCI is already going on, coordinated by the Commission in the case of the terrestrial segment, and ESA in the case of the space segment towards operational quantum key distribution (QKD) services, a highly secure form of encryption. The EuroQCI will make use of innovative quantum communication technologies developed by the researchers of the EU-funded Quantum Technologies Flagship.

Funding for the EuroQCI is being provided by the Digital Europe programme (https://digital-strategy.ec.europa.eu/en/activities/digital-programme) and the Connecting Europe Facility (https://digital-strategy.ec.europa.eu/en/activities/connecting-europe-facility), as well as Horizon Europe (https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en), ESA, and national funds, including the Recovery and Resilience Facility.

According main press releases in 2021-2022, the Digital Europe programme provided funds support for:

• the development of European QKD devices and systems

• the development and deployment of national quantum communication networks

• a testing and certification infrastructure for QKD devices, technologies and systems that will ultimately be used in the EuroQCI.

In 2022-2023, the Connecting Europe Facility provides funding support for cross-border links between national quantum communication networks, along with links between the EuroQCI's earth and space segments.

EuroQCI: digital europe call for a quantum communication infrastructure.

Funding budget provides 20 million euros available to develop, at national level, systems and networks that can test quantum communication technologies, with the aim of integrating them with existing communication networks and supporting the European Quantum Communication Infrastructure (EuroQCI).

3.5 Chinese Quantum Communications research a deployment plans

Source:

https://phys.org/news/2021-01-world-quantum-network.html

In 2021 the official announcement :

"Chinese scientists have established the world's first integrated quantum communication network, combining over 700 optical fibers on the ground with two ground-to-satellite links to achieve quantum key distribution over a total distance of 4,600 kilometers for users across the country

Using trusted relays, the ground-based fiber network and the satellite-to-ground links were integrated to serve more than 150 industrial users across China, including state and local banks, municipal power grids, and egovernment websites"

3.6 Quantum Communications Research & Deployment plans in Russia

On July 13th 2023, major russian scientists took part in the Future Technologies Forum "Computing and Communication. Quantum World", an annual event

on the main trends in science and technology took place on July 9-14 in Moscow, bringing together international scientists, experts and business managers of major industries in Russia working on the creation and implementation of solutions based on quantum technologies.

The key theme of the conference is Artificial Intelligence and QuantumTechnologies. Putin opened the forum with a speech on the potential ability of these technologies to determine the future of the country and to strengthen Russia's technological sovereignty. For this purpose, a program of research funding has been prepared to support Research and Development plans on the topics of #QuantumComputing, #QuantumSensing and #QuantumCommunications.

Finally, during his speech, Putin underlined Russia's willingness to attract researchers, including foreign ones, with the aim of creating synergies between the academic world and the industrial world and promoting training courses of excellence on the Quantum theme.

Source:

https://sputnikglobe.com/20230714/future-technologies-forum-russia-races-against-timepushingquantum-computing-1111878551.html

References

[1] Giovanni Gasbarrone, "Digital Transformation and Industry 4.0", in IoRoma ,

-https://rivista.ording.roma.it/industry-4-0-come-la-digital-transformation-incide-nellarivoluzioneindustriale/

[2] Giovanni Gasbarrone "On 5G in a post pandemic world", IOTHINGSMAG,

- http://www.iothingsmag.com/5g-e-sicurezza/

[3] Giovanni Gasbarrone "5G -Smart Working " Agenda Digitale- 5G cosa cambia per il mondo del lavoro"

https://www.agendadigitale.eu/infrastrutture/5g-cosa-cambia-per-il-mondo-dellavoro/

[4] Giovanni Gasbarrone "INDUSTRY 4.0" 5G e Industria 4.0, il ruolo delle TELCO per la quarta rivoluzione industriale :

https://www.agendadigitale.eu/infrastrutture/5g-e-industria-4-0-ecco-il-ruolo-delle-telco-perlaquarta-rivoluzione-industriale/

[5] Giovanni Gasbarrone "Cybersecurity a prova di 5G, così nasce la resilience by design"-

https://www.agendadigitale.eu/infrastrutture/cybersecurity-a-prova-di-5g-cosi-nasce-laresiliencebydesign/

[6] Giovanni Gasbarrone "Cybersecurity per IoT e 5G, il ruolo strategico degli standard"-

https://www.agendadigitale.eu/sicurezza/cybersecurity-per-iot-e-5g-il-ruolostrategicodeglistandard/

[7] Giovanni Gasbarrone "Cognitive Radio and Software Defined Radio for Telecommunication networks " in IoRoma , technical magazine - Ordine Ingegneri di Roma

https://rivista.ording.roma.it/cognitive-radio-e-software-defined-radio-per-le-reti-ditelecomunicazione/

[8] Giovanni Gasbarrone "5G and IoT to manage electricity grids: the impact on cybersecurity" 5G e IoT per gestire le reti elettriche: l'impatto sulla cybersicurezza (anche delle auto) – Agenda Digitale

https://www.agendadigitale.eu/infrastrutture/5g-e-iot-per-gestire-le-reti-elettriche-limpatto-sulla-cybersicurezza-anche-delle-auto/

[9] Giovanni Gasbarrone "Towards 6G: models and strategies for the Italian and EU ecosystem

https://www.agendadigitale.eu/infrastrutture/verso-il-6g-modelli-e-strategie-per-lecosistemaitaliano-e-ue/

[10] Giovanni Gasbarrone - Advisory Board IOTHINGS World (Advisory Board – IOTHINGS World)

http://www.anutei.it/index.php/8-conferenze/78-anutei-all-iothings-2023

[11] Giovanni Gasbarrone - The "Quantum" evolution in the future of the development of Telecommunications and Radar

http://www.anutei.it/index.php/corpo-ingegneri/72-l-evoluzione-quantistica-nel-futurodellosviluppo-delle-telecomunicazioni-e-nei-radar

A Military Gamification Model

Ph.D. Candidate, Adriano Pantaleo

Department of education sciences, human sciences and intercultural communication

Siena University

for

NATO CA2X2 FORUM 2023 LIVE EDITION (3-5 OCTOBER 2023)

Theme: M&S as a Cross Functional Enabler

Topics: Education & Training , Defense University M&S research

Abstract

As technology continues to innovate, training and education always seem to chase after the acquisition and diffusion of new skills involving human computer interaction. In this paper as a contribution in solving the training/ educatio nal problem of military contexts about the lack of a culture of failure and the need of superior approval reported in a previous NATO CA2X2 paper produced by Wolfhard Schimdt, military gamification is proposed.

Military gamification is a predictive research product generated through a correlational study between the game based motivational design elements belonging to Chou's 2015 Octalysis model and the military motivational factors belonging to Pakozdi and Bardos 2022 pyramid model. The military gamification model presented is intended for the design and analysis of military training/training/education experiences.

***KWs**: gamification; learning motivations; education; training; military.*

***Target**: personnel employed in military contexts, both military and civilian.*

***Research question**:*

- What elements of gamification could significantly affect educational and/or training motivations in a military context?

1 Gamification

Discovering the most effective teaching/learning dynamics has always been an area of a deep scientific interest as the amount of information and data to be acquired grows relentlessly in tandem with technological advancement, while the amount of time allowed for study is increasingly reduced due to the principles of competition ruling today's professional world.

As of 2010, one of the learning methodologies that has become of deep interest is the exploitation of game elements, regardless of the seriousness or formality of the application context. For example, the most recurring mechanic in learning how any new *software* works is the experience based on failure, called " *trial & error* ," a learning process peculiar to most of ludic activities.

The learning methodology involving the use of game ful elements in non game contexts is called in the literature "gamification," in the words of Mario Giampaolo, a *Game Base Methodology* (GBM)

<< *exploits the mechanics and dynamics that make games com pelling to motivate people*.>>

The term " *Gamification* " turns out to have been coined in 2002 by *game designer* Nick Pelling, and there are as many definitions clearly influenced by the professional background, among which the most famous and reused one belon gs to Deterding et al. (2011). During his studies and research on human computer interactions, he came up with the following definition:

"*Gamification is defined as the use of game design elements in non game contexts*."

To date, applications of *gamification* for adults can be found in various fields, such as in corporate training, health management, sports, educational activities, psychological training, and digital training and others.

Gamification is a possible innovative solution tool for professional context that lacks in the culture of failure since the freedom of failure is the most significant principle of a gamification design In fact, the following are the most valuable and validated design principles exposed in literature for a gamification learning environment environment[1]

- freedom of failure;

- speed of feedback;

- sense of progression;

- incentives and recognition;

- narrative.

2 Motivational Factors

Among the most widely accepted motivational theories for educational design and analysis of gameful learning experiences is A.H. Maslow's pyramidal hierarchy. According to A.H. Maslow's theory, first published in 1943, human beings satisfy their needs according to a hierarchy, which has as its base physiological needs, thus primary, and, ascending, incr easingly complex and abstract needs such as self actualization. The main feature intended to explain the hierarchical form consists in the impossibility of satisfying the highest needs if the basic needs, as outlined below, are not satisfied first:

[1] Dichev, C., Dicheva, D., Angelova, G., & Agre, G. (2014). From gamification to gameful design and gameful experience in learning. Cybernetics and information technologies, 14(4), 80-100.

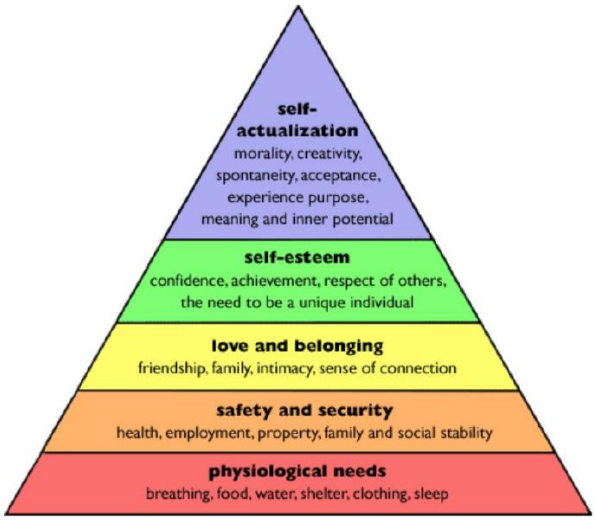
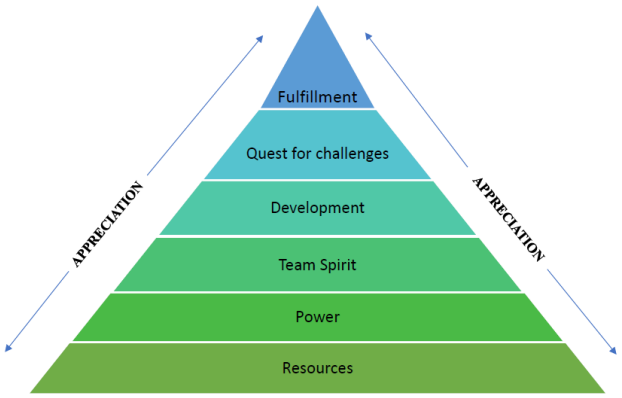


Image source: https://www.researchhistory.org/2012/06/16/maslows hierarchy of needs/

The translation of this pyramidal motivational model for a military context was carried out by Pakozdi and Bardons in 2022.

Building on Maslow's pyramid model, Pakozdi and Bardos in 2022 published the results of their research conducted at the *Hungarian Defense Forces Forces*[2] to develop a pyramid model adapted to the military context related to personnel who had already been enlisted for at least five years. By analyzing and cod ing the collected data, the researchers produced the military needs pyramid structured as follows:



In particular:

- Resources as security demands, such as job and social position, lifestyle, and family arrangements, which serve to counterbalance factors due to the military environment such as insecurity about professional future and uncompetitive pay. Resources as personal beliefs given by the culture of the military organization, such as training notions, patriotism, courage, professionalism, humility, pride, resilience, honor, and a sense of having a purpose. Resources also understood as health expectancy and athleticism.

- Power, understood as a soldier's ability to perform what is required. The ideal soldier is creative, adaptive and committed to national defense by serving with vitality and ascendancy in both war and peace operations. Power understood as the ability to self-control and self-empower oneself on a daily basis to provide for the safety and security of one's country.

- Team spirit, translatable as esprit de corps, understood as the sense of belonging to the deeper meaning of feeling like a second family. The phrases "we are a team" and the word "togertherness" characterize military motivation at both the individual and organizational levels. Esprit de corps such as camaraderie and being a comrade are two other terms that well identify the feeling of mutual support no matter what.

- Development, as the need to adapt to an environment characterized by a changing perception of security. Development as the desire to learn a foreign language or to understand how a new technology works. New assignments generate experience and knowledge gained through lifelong learning. The love of learning is the basis by which we change and develop, a need found in many interviews.

- Quests for challenges, includes training, career continuation, and testing one's limits. Varying goals

[2] Pákozdi, M., & Bárdos, G. (2022). A new military hierarchy of needs model. Social Sciences, 11(5), 217.

and assignments are also part of this motivational plan, where creative thinking is associated with combining what has been learned and experienced.

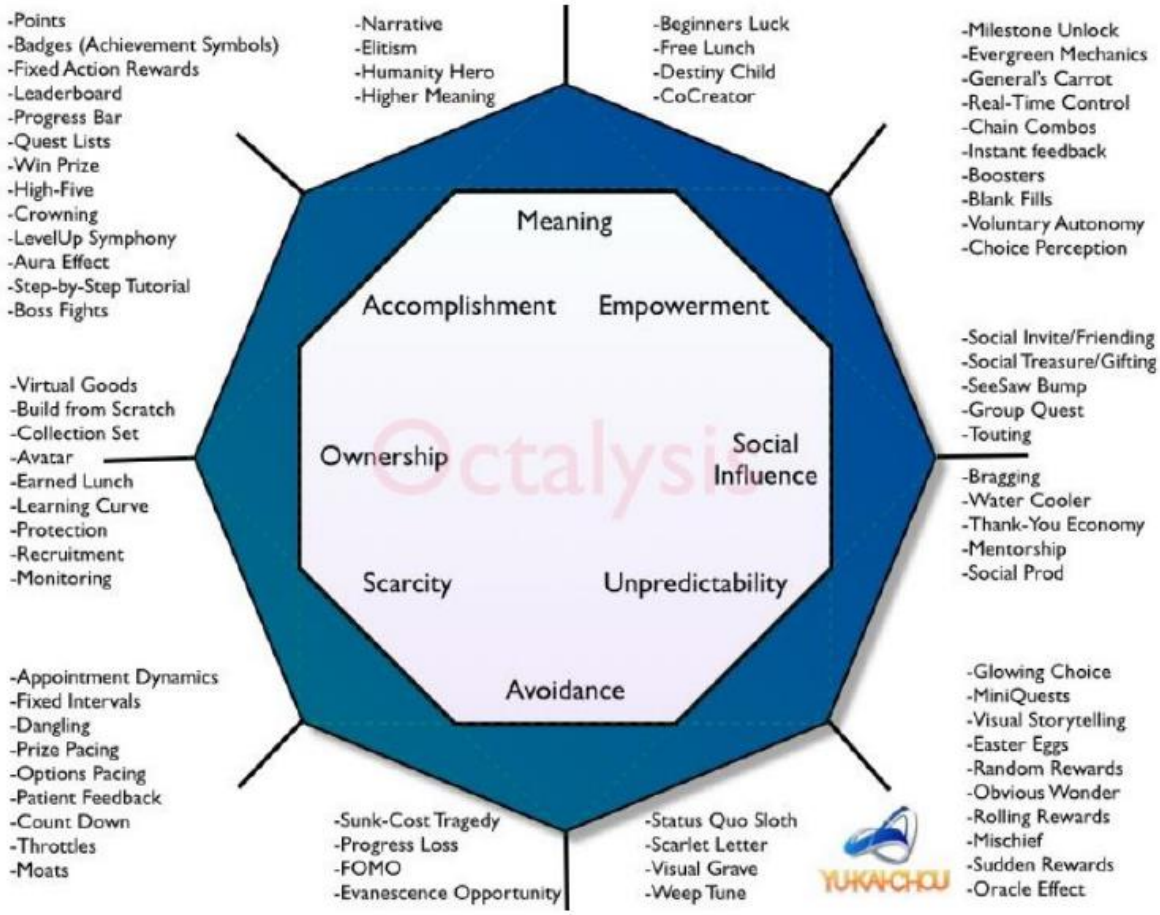
- Fulfillment, understood as a sense of living a meaningful life doing what one enjoys doing. Elements of fulfillment are being in service for good pay, loving the profession, giving security to the family. This feeling of fulfillment involves creating new thoughts and solutions by facilitating military service as well.

- Appreciation. This is primary need among all military personnel. Feeling appreciated by one's fellow soldiers and society is the most satisfying recognition a military person can experience. The author concludes that for a military member to feel unappreciated involves negative emotions holistically and is something they hope scientific research will continue to explore.

- To leverage what is scientifically produced by the military motivational schema and gamify the education/training in a military context, it becomes necessary to understand what game elements might satisfy these military motivational needs. In other words, to find out what gamification design elements embedded in a military context allow for greater individual involvement and engagement with the aim of achieving greater results from training and educational experiences.

3 The "Octalysis" Motivational Gamification Model.

In 2015, a milestone in what to this day continues to be a world renowned model for *Gamification* was being published in his book by Yu Kai Chou, an entrepreneur who has risen to stardom through his passion for making as much of life a game as possible. In particular, his most noteworthy and undisputed work among *Gamification* experts is the *Octalysis* model. A model that breaks down and encapsulates into eight motivational cores the mechanics that transport a person to game and keep him playing.



3.1 Core Drive 1: *Epic Meaning & Calling*

The first motivational core can be translated as the epic significance and vocation. In other words, the participant must feel that he or she is the chosen one who is going to perform actions beyond his or her own exis tence. An example Chou brings up is *wikipedia* , where the user contributes to the online encyclopedia with a higher purpose in mind, which in this case it might be preserving human science. Instead, this leverage can also be activated in a more circumscribe d way, and a common case is described, namely when the game allows an event to happen as a stroke of luck, so called " *beginner's luck* ," causing the participant to feel better than others or otherwise part of a unique and irreproducible experience path.

3.2 Core Drive 2: *Development & Accomplishment*

The second motivational core is defined by Chou as the internal drive in progressing, developing skills, mastering and overcoming challenges. Chou highlights how this kind of drive can be easily designed by servi ng Points, Recognitions and Rankings.

3.3 Core Drive 3: *Empowerment of Creativity & Feedback*

The third motivational core is activated by creativity and by feedback derived from actions. Chou asserts that people need to express their creativity and at the sa me time encounter the results produced to adjust their focus. Lego in and example representing an Evergreen Mechanichs ". These are mechanics that ideally will never stop working because the mind independently produces fun with what it has just produced in a potentially endless cycle.

3.4 Core Drive 4: *Owership & Possesion*

The fourth motivational core is driven by ownership and possession. Chou explains that any person is by nature motivated to improve what he or she owns. The example taken from games is that of avatar customization and the accumulation of virtual goods ; the more time a person invests in something, the more his or her motivation to own and improve that something increases.

3.5 Core Drive 5: Social Influence & Relatedness

The fifth motivational core is driven by social influence and relatedness. Thus, according to Chou, all emotions that arise from social interactions, such as envy or admiration, and anything that stems from a feeling of connectedness, such as nostalgia for a memory or hope for the fulfillment of a desire, generate motivation to be involved and engaged.

3.6 Core Drive 6: *Scarcity & Impatience*

The sixth motivational core is generated by the sense of scarcity and impatience. Chou explains the sense of scarcity as the simple desire to have something rare, exclusive or unobtainable in the immediate fut ure. The author gives the example of Facebook, which waited a longer time than expected before opening its doors to the world.

3.7 Core Drive 7: Unpredictability & Curiosity

Chou's seventh motivational core is activated by the occurrence of unpredictable events, since the mind when it perceives something unusual raises its level of attention by a large amount. As an example, addiction to gambling or lottery and the like is highlighted, where inevitably the happenings are unpredictable. The author concludes with another example that activates this core although

in a less impactful way: reading a book or watching a movie.

3.8 Core Drive 8: Loss & Avoidance

The last motivational core is defined by Chou as the most obvious because it is activated by the will to avoi d negative happenings. The examples he gives are the will to avoid a change in work or habits, and, more deeply, the will not to admit that one has made a mistake. Chou concludes, one finds the use of this core drive in conveying the feeling of missing an opportunity.

4 A Military Gamification

By relating the pyramid as a motivational system in a military context to Chou's motivational cores, it is possible to infer that:

- The mechanics gathered under the *core drives of Ownership and Avoidance* are connected with Resources/Resources

- Related to *Power/Power* are the mechanics of *Empowerment and Meaning*.

- Related to *Body Spirit/Team Spirit* are the mechanics of *Social Influence*.

- Related to *Development / Development* are the mechanics of *Accomplishment and Empowerment*.

- Related to the *Request for Challenges / Quest for Challenges* are the mechanics of *Accomplishment and Empowerment*.

- Related to *Self-Realization/Fulfillment* are the mechanics of *Meaning*.

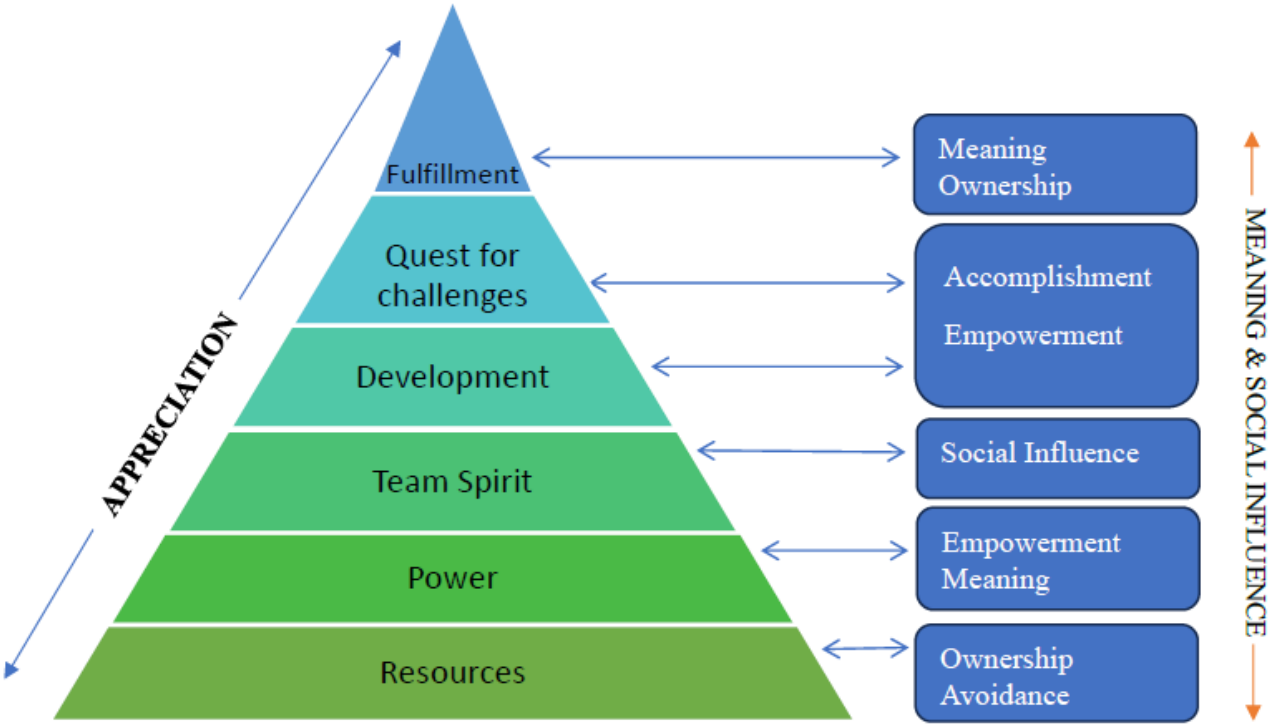
- Since *Appreciation/Appreciation* is a holistic need in a military context, the mechanics gathered under the core drives of *Meaning and Social Influence* might result in a remarkable effect in terms of engagement and motivation at any time in any type of training/training experience.

- The *core drive Avoidance*, as well as being at the base of the pyramid should always be considered throughout the *gamification* experience since the sense of loss is very important in a military context.

- Finally, note how the *core drives* of *Unpredictability* and Scarcity do not appear to be included in the connections between military motivational factors and *Gamification* mechanics.

This final peculiarity could be due to the fact that in the military world there is always an attempt to avoid the surprise factor or *Unpredictability* , since it is a bearer of un desired risks, and it is a generator of events that are not quickly manageable . Whereas, as for the absence of the *core drive Scarcity*, it may make sense since in the military world what turns out to be rare/unique or presented late might arise an anti ethical social effect, rather than generating suspense and/or desire. In any case, their absence from the main connections above does not mean their exclusion from an analysis or design of a *gamification* experience in a military context.

Below is a summary diagram of the correlation between the *Octalysis model* and the pyramid model of military motivation:



Not only that, but the pyramid model also represents the type of connection between the needs sought in a military context, i.e., the first need *resources* is at the base of the pyramid, therefore, it will be the first need to be satisfied and then, following that, comes the satisfaction of the other needs. Then, bringing this kind of connection on a *gamification* experience it becomes important to have mechanics encapsulated in the *core drive* of Chou *Ownership & Avoidance* since the beginning. Thus, through this correlation it is also possible to leverage the hierarchical model of needs also as an index of priority and importance of gamification elements used to analyze or design a training/educational activity.

Hence, examples o f desirable elements of the *gamification Octalysis model* to be used in a military context in order of priority and importance are:

1. Design elements of Ownership & Possesion such as:

O *Build-From-Scratch*. Allowing participants to customize their experience from the initial stages activates what is named by the behaviorist researchers Dan Ariely and Mike Nortono: the "*Ikea Effect.*" In other words, customizing facilitates attachment to the *gamification* experience as soon as it starts. Some examples on *online* educational experiences might be the personalization of one's avatar or a virtual room; in an *analog-offline* experience it might be the initial free choice of materials to bring along or the choice of an alternate name and personal/group motto.

O *Collection Sets*. Giving the opportunity to accumulate collectibles is an influential game mechanic on the sense of ownership and possession. Collectable could be virtual and/or real objects.

O *Exchangeable Points*. A *gamification* dynamic that connects very much with social interaction. Particularly effective if there subsists both a points or collectibles system; moreover, a long-term effect could be reach if there subsists a savable points or collectibles system such that there can be exchanges with those who have already participated in the *gamification* experience.

O *Monitor Attachment*. It consists of the participants' intention to check/monitor the progress of statistics

or other values. It can take the form of a *dashboard* or, otherwise, a constantly updated summary chart on the progress of the training/educational experience.

O The *Alfred Effect*. The *Alfred Effect* is when personalization reaches extreme levels, such as the personalized tv-choices based on past choices of TV Series or Movies, examples are TV-applications such as Amazon Prime or Netflix operate. Its already complex usage in digital applications makes this effect more unlikely for analog or otherwise offline *gamification* experiences.

2. Design elements of Loss & Avoidance such as:

O *Rightful Heritage*. It consists of conveying a sense of loss through the bestowal or accumulation of temporarily fictitious assets, which materialize only upon the performance of a specific action at a specific time in a specific place. A commercial example is personalized time offers; a financial example could be the pension system.

O *Evanescent Opportunities* and *Countdown Timers*. These are design elements that serve to convey a sense of urgency and priority. The first is a dynamic generated by extemporaneous, random and perhaps unrepeatable happenings, such that we tend to focus exclusively on the luck of what is happening and let everything else out of focus. The other, is the known mechanics of the countdown; highlighting how much time is left until an offer expires conveys a sense of urgency in taking the desired action. Competitive bidding/applications are a public administration example pertinent to these dynamics/mechanics.

O Status Quo Sloth and FOMO Punch (Fear Of Missing Out). The first dynamic corresponds to resistance to change due to investments made in something; the second dynamic, as a counterpart, corresponds to the fear of regret. The former is good to exploit toward the end or in a repetition of the gamification experience; the latter is best exploited at the start of the education/training experience in order to have a good initial motivational momentum.

O *The Sunk Cost Prison*. This motivational dynamic is perhaps the most powerful, as it is realized through the investing of time and energy; even though something is no longer enjoyable, one continues to pursue it just so as not to feel the sense of loss that would result from quitting. Accumulating something during the *gamification* experience such as collectables, *status*, rewards, trophies, progress, relationships, involves activating this motivational system.

3. Design elements of *Social Influence*:

O *Mentorship*. On the one hand it helps novice participants to be included and supported, and on the other hand it helps veterans or instructors to maintain a high level of importance and involvement.

O *Brag Buttons* and *Trophy Shelves*. *Brag buttons* are actions one can take to spread/expose, then brag, about one's achievements. While the *trophy shelves* mechanic is a passive exposure of one's achievements, such as setting up a shelf or a wall of trophies and accolades.

O *Social Treasure*. These are awards or gifts that can only be received by co-participants.

O *Social Prods*. These are mechanics that involve non expensive action to generate free or maneuvered social interaction through preset messages.

O *Conformity Anchor*. A motivational *gamification* dynamic that is established with the perception of a social normality to conform to.

O *Water Coolers*. It consists of designing a time when you can take a break so that you can spar about what is going on. Any online forum is an example.

4. Design elements of *Empowerment & Feedback* such as:

O *Boosters*. Different from raising difficulty or using new skills, boosters are temporary facilitators that can be activated on certain conditions.

O *Milestone Unlock*. These are particular unlocking moments from which participants could pause the

experience to return to the initial exercises, because the previous exercises/levels are easier to complete thanks to what they have just unlocked.

O *Choice Perception*. Mechanisms that let participants perceive that they can choose what to learn first or later, or what to exclude from their experience. In the design work, it is important that it remains a simple perception by which the educational/training objective is pursued without distraction.

O *Meaningful Choices*. They correspond to choices that influence the course of the educational/training experience. The main differentiation of meaningful choices was expounded by Jesse Schelle, who explains the importance of allowing participants to be able to choose for themselves whether to go down a risky path but one that could yield a great outcome, or a path that is less risky but involves a less prestigious outcome.

5. Design elements of *Accomplishment & Development* such as:

O Progress bars, particularly simple but effective. They can be settled in an *online* training environment or can be integrated into a blended/analog training/educational environments.

O *Rockstar* effect involves designing an activity in which participants feel particularly wanted and desired.

O Symbols, such as *badges*, trophies, belts, medals any object that symbolizes the achievement of a goal.

O *Status* points may be points related to the progress of the experience or skills acquired, or still may refer to both. In this way, both participants and instructors can know the overall progress in the training/educational experience.

O *Leaderboards*. Leaderboards/rankings are an element of gamification that can easily have motivational repercussions. It is important not to let new participants see the huge gap that might be with the front-runners, but only to be aware of their scoring zone or their initial placement in niche leaderboards. Another important mechanism is a continuous reset of the rankings so that participants are constantly stimulated to maintain or obtain top positions.

6. Elements of *Meaning & Epic Calling* such as:

O Narration, how to save someone or the world.

O Heroism, such as helping to solve a case as part of a humanitarian or charitable mission.

O Elitism, as the exaltation of one or more groups.

O *Beginner's luck*, making the experience unique with events dictated by a "design destiny".

O *Free Lunch*, how to bestow any kind of reward related to a charitable action.

In conclusion, a few general recommendations extracted from the literature[3] which could be useful as guidelines for *gamifying* an educational/training experience in a military context:

- Having conducted a training needs assessment of a specific and identifiable problem/gap; assessing on what to intervene such as reactions, outcomes, ROI (Return Of Investment) in the form of *military readiness*, or other factors deemed important as an outcome of the training.

- Gamifying an already effective training could make the results worse.

- Content and methods are to be gamified out one at a time.

- You can gamify even just one piece of content or even just one method, such as using a *storyline* instead of a *PowerPoint* presentation.

5 Theoretical Limits of Military Gamification

[3] Landers, R. N., Auer, E. M., Helms, A., Marin, S., & Armstrong, M. B. (2019). Gamification of adult learning: Gamifying employee training and development. The Cambridge handbook of technology and employee behavior, 271-295.

The proposed theoretical inferences are of desirable application for military personnel already professionally embedded in military contexts; but may not necessarily be effective for civilian personnel even if embedded in a military work context.

The military motivational pyramid does not consider particular categories, such as gender, age or other individual identity elements. Moreover, it is a model still in the process of validation.

The *Octalysis* model often refers to digital/virtual *software* and applications in commercial and entrepreneurial contexts . Although this paper provide s a first attempt of a recontextualization other studies are needed for the military context

Designing a training/educational activity using *Gamification* may be inaccessible to a trainer unfamiliar with game design ; therefore , training for teachers may be required before full advantage can be taken of *Gamification* experiences aimed at traine e s/learners.

Gamification to be implemented as an innovative solution aimed at developing a culture of failure for a military context requires long term planning and a wide reach; occasional, circumscribed attempts are unlikely to carr y out cultural change within any large organization as well as a military context.

The examples given as design elements of *Gamification* count as explanatory but not exhaustive examples. The landscape of *gamification* mechanics and dynamics has a scope that is difficult to define; any list proposed by experts and researchers remains expressed as a mere stance.

6 Conclusions

The use of educational/training learning environments designed with *gamification* elements is widespread as a type of guideline for designing software or applications, more generally for virtual environments. Research and experimentation regarding the use of purely analog or blended *gamification* elements are underdeveloped; the military context could be an environment for useful application and development of a *blended*-analog gamification.

For already enlisted military personnel, learning about *Gamification* may prove to be an awareness gain about established institutional motivational systems such as the use of badges, medals, and rankings. Regarding new recruits, there is evidence that new generations need different learning strategies than traditional ones, so experimenting a gamification design for initial training/education experiences could bring a significant increasement of the desired outcomes.

Among the modes of delivery of training activities designed with *Gamification*, optional participation is taken for granted, as it can be likened to a game activity. In an organizational-institutional, as well as military context, cultural changes are assumed to be likely by investing in newcomers, or by implementing training to already employed personnel through coercive persuasion. Therefore, when experimenting with a *gamification* experience that has as its purpose a cultural change trigger, it may be necessary to go against the odds and consider collecting data on a gamification learning experience proposed as a compulsory/necessary activity, inconvenient to avoid.

Bibliography

- Dichev, C., Dicheva, D., Angelova, G., & Agre, G. (2014). From gamification to gameful design and gameful experience in learning. *Cybernetics and information technologies*, 14(4), 80-100.

- Landers, R. N., Auer, E. M., Helms, A., Marin, S., & Armstrong, M. B. (2019). Gamification of adult learning: Gamifying employee training and development. *The Cambridge handbook of technology and employee behavior*, 271-295.

- Chou, Y. K. (2019). Actionable *gamification*: Beyond points, badges, and leaderboards. Packt Publishing Ltd.

- Wolfhard Schmidt, "Training and Education" panel, published in 2020, NATO Modelling and Simulation Centre of Excellence, Forum CA2X2 del 2020. link: https://www.mscoe.org/document/nato-ca2x2-forum-2020-papers-collection/

- Pákozdi, M., & Bárdos, G. (2022). A new military hierarchy of needs model. *Social Sciences*, 11(5), 217.

What Can, What Could, What Should…

…Simulation Supporting Delivery of Enhanced Effectiveness of JFS Training in a Live Environment?

Advancements in Indirect Fire Simulation with Modern Weapon Systems: Leveraging Live Virtual Constructive Environments for Enhanced Military Training-

Abstract

In a current research & technology assignment the potential of an advanced simulations and debriefing software is being investigated, derived from an integral component of numerous NATO (Air Defender, TREX…) exercises and the Joint Terminal Attack Controller (JTAC) training provided to the German armed forces. The software, characterized by its precision-based modeling of weaponry and environmental contexts, providing a heightened fidelity in indirect fire simulations involving modern weapon systems. The largest and currently sole use in military training takes place in air-to-air-combat-training. While enhancing the potential in this field, the use of the software in Joint Fire Support (JFS) training missions, such as air-to-ground-training, ground-to-ground-training, and the combination of both is at the moment not used to its full potential. The exploration focuses on the software's ability to accurately depict a variety of weapon systems and the inherent complexities in indirect fire situations with all environmental aspects accounted for.

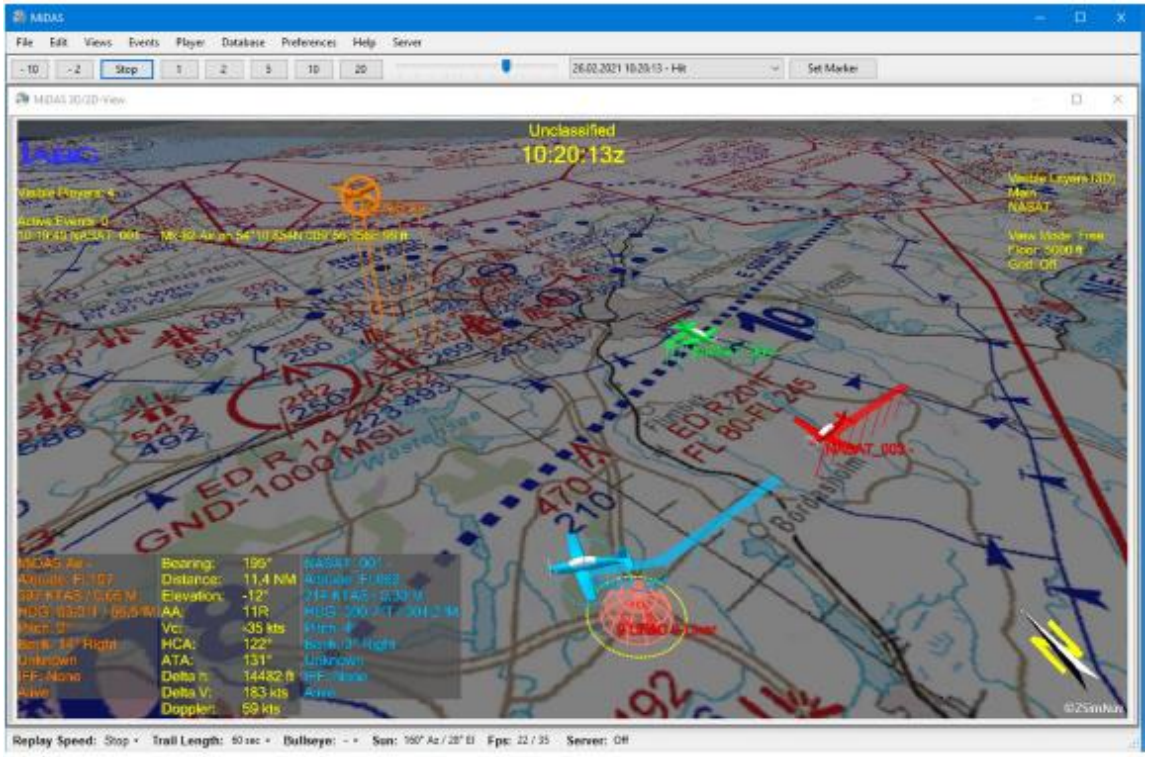


Figure 1: Screenshot MIDAS simulated Employment of MK-82 Airburst

The research also highlights the pivotal role of the software in fabricating live, virtual, constructive environments, a necessity for engendering authentic, efficient training experiences. This parallels its proven effectiveness in JTAC training and extends its application to the realm of joint fires. The software's capability in enriching debriefing sessions, facilitating comprehensive performance reviews, and thereby streamlining training

optimization is also elaborated, leveraging its practical application and the proven track record with the German armed forces to underline the improvement in operational readiness and training efficiency. By enabling multiple players, both air-based and ground-based to visualize following possible items: the flight path of the aircraft (Figure 1), deconfliction of all players (Figure 3) (vertical, lateral, and timely), the weapon-delivery-trajectory (Figure 2) from point of origin to point of impact and the dome of a weapons effect (Figure 1 and Figure 2), you enhance situational awareness of the trained military personnel while debriefing. Thus, debriefing is brought to a significant detailed level and the invested time in military training is used more efficiently.

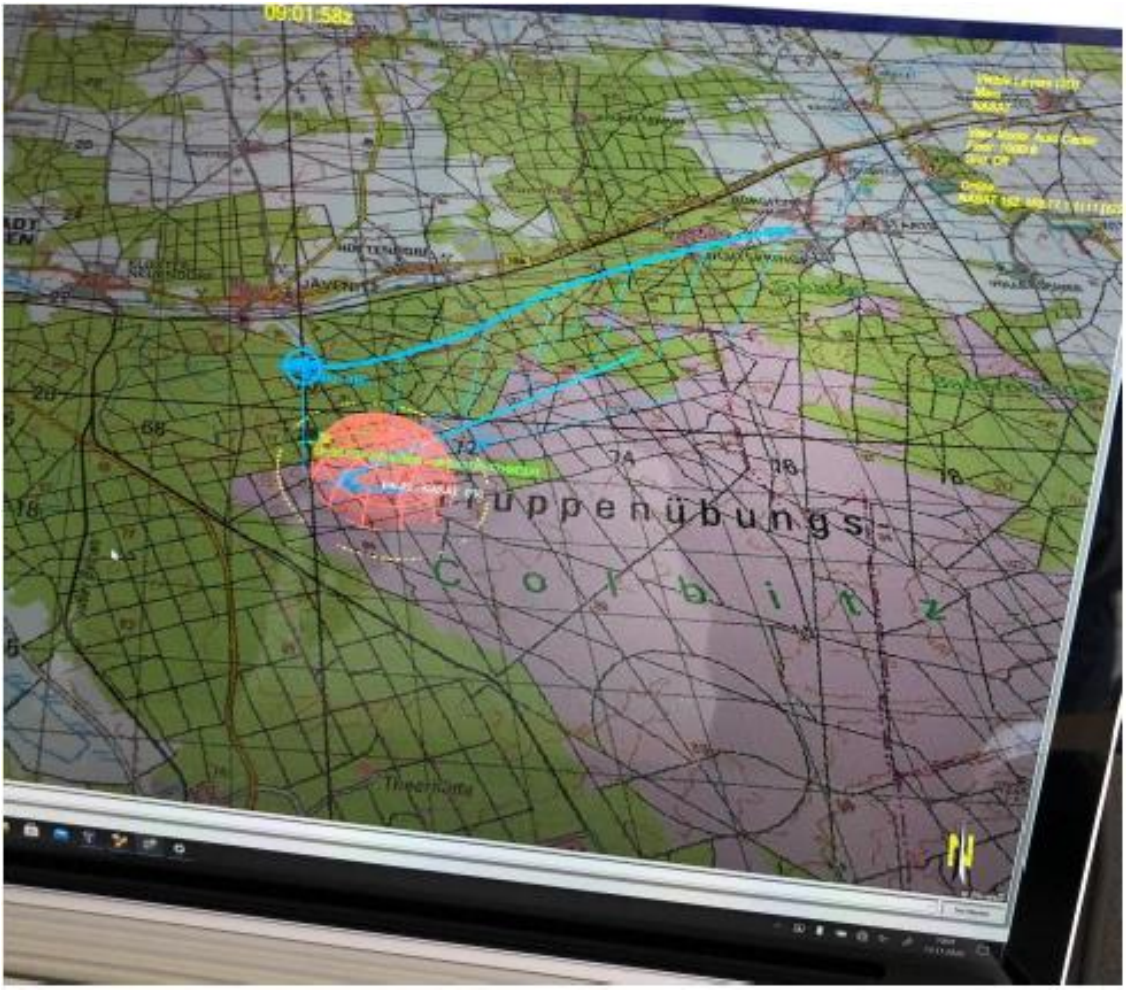


Figure 2: Weapon-delivery-trajectory (Blue Arrow)

The advantages of Live Virtual Constructive environments, such as cost-effectiveness, adaptability, and scalability, are discussed in the context of JFS training. A significant decrease in costs is possible by implementing LVC environment

.

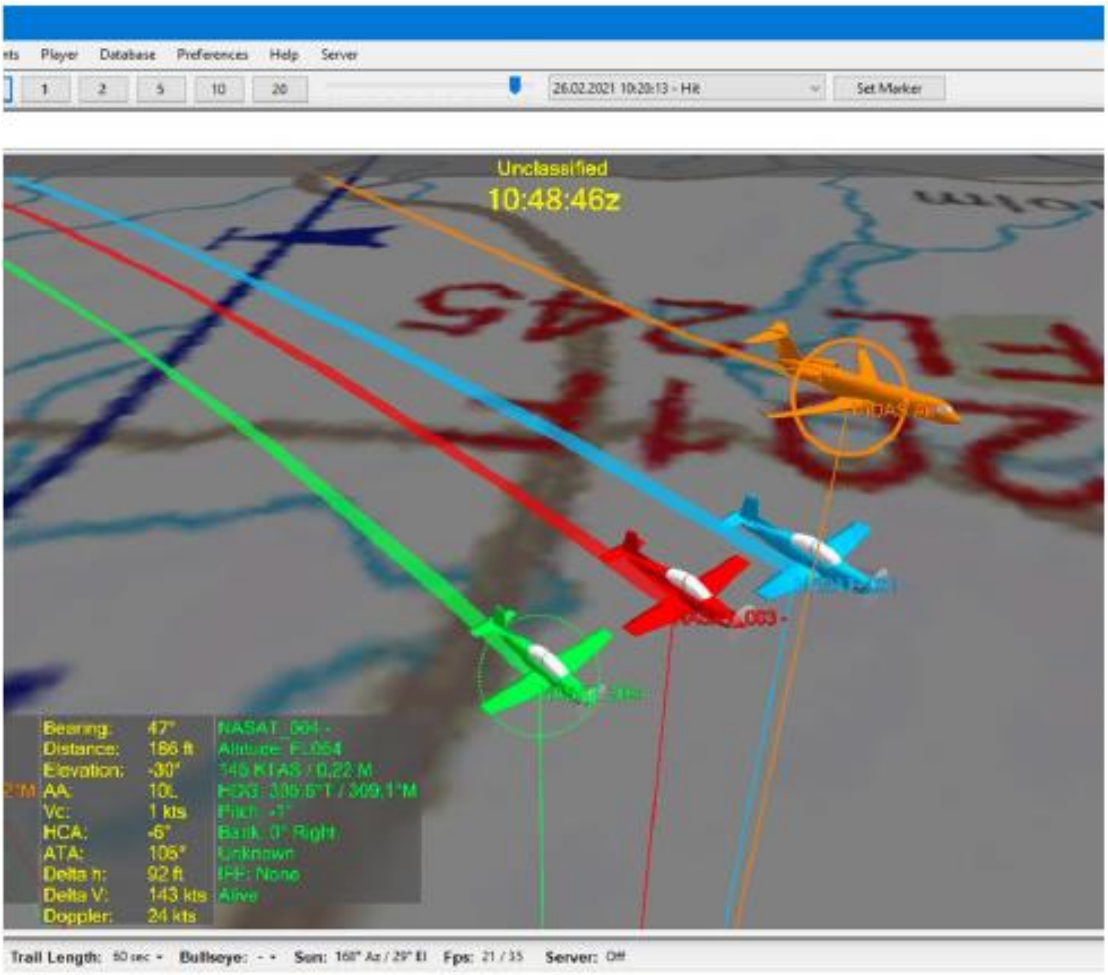


Figure 3: Visualization of Deconfliction of multiple A/C

Furthermore, the paper examines case studies of military organizations that have successfully incorporated LVC-based Joint Fires simulations into their training. These case studies underscore the effectiveness of this approach in enhancing decision-making, strategic planning, and tactical execution in simulated Joint Fires scenarios.

Additional elements and features are:

- *The ability to handle several TDLs like Link16, (SIMPLE, JREAP-C), Asterix, CESMO, and Protocols like NMEA and potentially VMF which is giving the opportunity for…*

- *…the integration of upcoming procedures like DaCAS*

The research and development highlight the need for accelerating the Technology Readiness Level (TRL) of this software to fully harness its potential. The imperative role of community contributions is underscored for outlining the requirements necessary to attain this escalated TRL, keeping in mind the multifarious needs and prerequisites of all stakeholders. It is foreseen to be a collaborative effort, blending the expertise, cognizance, and perspectives of diverse participants to materialize a more evolved, potent tool.

In conclusion by extending an invitation for open discussions and inviting the community to share their insights, experiences, and innovative ideas to further augment this software's capabilities. Such concerted participation will pave the way for a new epoch of technologically sophisticated military training, bolstering preparedness and operational efficiency on an international scale.

Talk about us

Italian Ministry of Defence

www.difesa.it

Telegiornale 2

rainews.it

NATO Allied Command Transformation

act.nato.int

/article/digital-transformation-at-coe-annual-event/

NATO Science and Technology Organization

sto.nato.int

issuu.com/niva_inc/docs/nato-sto-cpow-2023

Advanced Distribute Learning Initiative

adlnet.gov

Centro Studi Internazionali

cesi-italia.org

/it/articoli/il-forum-ca2x2-e-la-nuova-generazione-del-nato-mands

---

Analisi Difesa

analisidifesa.it

/2023/10/a-roma-la-18a-edizione-del-ca2x2-organizzata-dal-centro-di-eccellenza-nato-ms/

Infodas

infodas.com

L'agone Nuovo

lagone.it

/2023/10/08/la-diciottesima-edizione-di-nato-ca2x2/

Castelli Notizie

castellinotizie.it

/2023/10/07/a-roma-tanta-meraviglia-per-la-18-edizione-del-nato-ca2x2-leccellenza-tecnologica-per-modelling-and-simulation/

Insider Trend

Insidertrend.it

/2023/06/29/difesa/difesa-nato-ms-coe

-il-comandante-del-sact-

in-visita-al-centro-di-eccellenza-della-cecchignola/

Monolite Notizie

monolitenotizie.it

/attualita/centro-di-eccellenza-nato-ms-organizza-

la-18a-edizione-del-forum-ca2x2/

/roma-e-provincia/top-di-capacita-tra-tecnologie-di-

modellazione-e-simulazione-ca2x2-forum-2023/

Congedati Folgore Giornale Quotidiano

congedatifolgore.com

/it/notizie-dal-centro-di-eccellenza-

nato-di-simulazione/

L'eco della pista

ecodellapista.it

Ecolago di Bracciano

ecolagodibracciano.it

/nato-ca2x2-forum-2023

-a-roma-successo-dellevento/

PART 1 — NATO M&S CoE Annual Review

- ELMO (Electromagnetic Layer for Multi-domain Operations) Developing and Testing Activities
- Modelling & Simulation in Support of a Comprehensive CBRN Layer Development
- Technical Report for AI/ML M&S Integration in Support of Decision Making
- WISDOM: The Development of a Wargaming Platform and its System Architecture

PART 2 — CA²X² Forum Paper Collection

- Cryptography within Critical Infrastructure
  Generative AI-Powered Live, Virtual, and Constructive Training Events
- Legal Roles in Exercises and Wargames
- "Quantum" Evolution in Europe
  The Future of Cybersecurity
- An Interoperable Generic Tool for Simulating Attacks within the Cyber Domain
- AI-driven Logistics Intelligent Decision Support (A-LIDS)
- Kubernetes as a SimaaS Platform
  Utilizing Containerization for Simulation Workloads
- Simulation-based Analysis of Dispatch Policies for Transportation in the Military Evacuation Chain
- 6G Technology Ecosystem Vision: a Dual Use Approach in Defence and Sovereignty of Countries
- A Military Gamification Model
- What Can, What Could, What Should…
  …Simulation Supporting Delivery of Enhanced Effectiveness of JFS Training in a Live Environment?

ISBN 979-12-985129-0-0

NATO
OTAN

MODELLING & SIMULATION
HONOS ALIT ARTES
CENTRE OF EXCELLENCE

www.mscoe.org