Vol. n. 1 • 2017 ISBN 978-88-942906-1-5

2017 Annual Review

NATO M&S COE

NATO Modelling & Simulation Centre of Excellence

2017 ANNUAL REVIEW

2017 ANNUAL REVIEW

NATO Modelling & Simulation Centre of Excellence

A NATO M&S CENTRE OF EXCELLENCE PUBLICATION

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

ISBN 978-88-942906-1-5 e-book edition

Printed in Italy.

Authors

MARCO BIAGINI, Concept Development & Experimentation Branch Chief,NATO M&S COE, Rome, Italy

ROBERTO CENSORI, M&S Service Branch, NATO M&S COE, Rome, Italy

FABIO CORONA, Concept Development Section Chief, NATO M&S COE, Rome, Italy

WALTER DAVID, Analysis & Lessons Learned Section Chief, NATO M&S COE, Rome, Italy

CHRISTIAN FAILLACE, Leonardo, Land & Naval Defence Electronics Div., Genova, Italy

SONIA FORCONI, M&S Enterprise Architect, NATO M&S COE, Rome, Italy

JASON JONES, Deputy Director, NATO M&S COE, Rome, Italy

MICHELE LA GROTTA, Support Branch Chief, NATO M&S COE, Rome, Italy

MARCO PICOLLO, Leonardo, Land & Naval Defence Electronics Div., Genova, Italy

ALFIO SCACCIANOCE, Experimentation Section Chief, NATO M&S COE, Rome, Italy

THOMAS LASCH, US Army/ Joint Multinational Simulation Center (JMSC) Grafenwoehr, Germany

CONTENTS IN BRIEF

Contents

LIST OF FIGURES

LIST OF TABLES

PREFACE

It is with great pleasure that the NATO Modelling and Simulation Centre of Excellence presents this, our first Annual Review. This Annual Review provides articles and summaries of selected research, studies and events that took place this year.

This review covers M&S work in the cyber domain, establishing an architecture for M&S as a service, implementing a lessons learned repository for M&S and an overview from our role leading the M&S Focus Area during NATOs Coalition Warrior Interoperability Exploration, Experimentation, Examination Exercise (CWIX).

As a NATO Centre of Excellence our very purpose is to support NATO and Nations in their transformation efforts by providing subject matter expertise in all aspects of Modelling and Simulation. This journal is prepared in that spirit, as part of our efforts to make our work more widely available and thus advance the capabilities of NATO, its Nations and partner nations, and the NATO M&S COE hopes it serves to further promote the sharing of information and ideas between NATO, the Nations and partners.

CAPT. (ITA NAVY) VINCENZO MILANO

Rome, Italy
September, 2017

ACRONYMS

AF	Armed Forces
BA	Baseline Architecture
CFBLNet	Combined Federated Battle Laboratories Network
CN&C	Communication, Networking and Cyber
COI	Community of Interest
ET	Exploratory Team
GIS	Geographic Information Systems
IAF	Italian Air Force
IDGS	Italian Defence General Staff
ITAR	Italian Army
ITB	Integration Test Bed
ITN	Italian Navy
JRR	Joint Radio Relays
LOS	Line of Sight
M&S	Modelling and Simulation
MPLS	Multi Protocol Label Switching
NEC	Network Enabled Capability
NFON	National Fiber Optics Network
NMRP	National Military Research Project
NMSG	NATO Modelling and Simulation Group
OR	Operational Requirements
OA	Overarching Architecture
OPNET	Optimized Network EngineeringTool

PoC	Proof of Conceptl
RA	Reference Architecture
ROIS	Radio to Optical Interface System
SACT	Supreme Allied Commander Transformation
TA	Target Architecture
TSE	Telecommunication Simulation and Evaluation
SITL	System in the Loop
TDM	Time Division Multiplexing
TNN	Telephone Numbering Network
TOR	Technical and Operational Requirement
UAxS	Unmanned Autonomous Systems

Part I

NATO M&S CENTRE OF EXCELLENCE

CHAPTER 1

OVERVIEW OF THE NATO M&S COE

1.1 The Centre

1.1.1 What is a NATO COE?

A NATO COE is an international military organisations that train and educate leaders and specialists from NATO member and partner countries. They assist in doctrine development, identify lessons learned, improve interoperability and capabilities, and test and validate concepts through experimentation. They offer recognised expertise and experience for NATO benefit and its Transformation, while avoiding the duplication of assets, resources and capabilities already present within the Alliance.

1.1.2 NATO M&S COE in details

- Accredited by NATO and Activated in 2012
- Italy is the Framework Nation with Czech Republic, Germany and the United States as Sponsoring Nations
- Established through Memorandum of Understandings (MOUs) between the participating nations
- Located in Rome, Italy

1.2 Mission

Our Mission is to support NATO and its Nations as well as participating Partner Nations by providing subject matter expertise on all aspects of M&S activities.

In discharging its mission, and as approved by the NATO M&S COE Steering Committee, the NATO M&S COE may also establish collaborative relationships with entities such as Industry, Academia and other organizations.

1.3 Our People

The NATO M&S COE invests in ts people in order to provide experts with reputable influence in NATO M&S Community of Interest (COI).
Its members are:

- Military members from 4 NATO Nations (CZE, DEU, ITA and USA) representing all military services;
- Experts in various combat and combat support roles;
- Experts in the application of M&S in support of military activities;
- Experienced military leaders and young 'digital generation' talents.

CHAPTER 2

NMSG ACTIVITIES

The NATO M&S COE contributes its expertise in the Technical Activities of the NATO Modelling and Simulation Group, a panel of the Science and Technology Organization (STO), the scientific organization of the North Atlantic Treaty Organization.

These Exploratory Teams (ET) and Modelling and Simulation Research Task Groups (MSG) bring together NATO and National experts from government, industry and academia to find solutions to complex issues for the alliance. Recognizing the potential value of these synergistic groups, the NATO M&S COE also invests its hardware, software and facilities to support their efforts.

The main activities are listed in Table 2.1.

Table 2.1 NMSG activities M&S COE is contributing to

Group	Description
ET 039	Operational Requirements for Training Interoperability.
ET 040	M&S Education and Training Curriculum.
ET 041	M&S for Acquisition.
ET 043	Hybrid Warfare Modelling and Simulationt.
MSG 127	Reference Architecture for Human behaviour.
MSG 134	NATO Distributed Simulation Architecture & Design, Compliance Testing and Certification.
MSG 136	Modelling and Simulation as a Service (MSaaS): Rapid deployment of interoperable and credible simulation environments.
MSG 144	NATO M&S Standardization.
MSG 145	Operationalization of Standardized C2-Simulation Interoperability.
MSG 147	M&S Support for Crisis and Disaster Management Processes and Climate Change Implications.
MSG 150	M&S Supporting Concept Development & Experimentation.
MSG 152	Establishing a Professional Modelling and Simulation Corps.

Part II

NATO M&S COE CD&E STUDIES AND EXPERIMENTATION

Selection of papers and documents

CHAPTER 3

COMMUNICATION, NETWORKING AND CYBER MODELLING & SIMULATION IN SUPPORT OF DEFENCE

SONIA FORCONI, MARCO BIAGINI

M&S Centre of Excellence

Translation by Maj. Paolo Cappelli, Italian Defence General Staff — V Div.

3.1 Executive Summary

This paper analyses the **Communication, Networking and Cyber Modelling and Simulation (CN&C M&S)** aspects that support technology innovation, modernisation, development, and acquisition of new capabilities across Defence. It will focus on:

- **Technology Innovation of Defence Strategic Network (TNN-NFON)** means modelling and simulation in support of the technical requirements that underpin the Technical and Operational Requirement (TOR) for the modernisation and rationalisation of the Telephone Numbering Network National Fibre Optics Network (TNN-NFON). The research methodology relies on the directives and guidelines issued by the 6th Division of the Italian Defence General Staff on the national Integration Test Bed (ITB) for the NEC Force Project, and on the outcomes of several TNN and NFON workshops. Through such methodology, a possible model supporting procurement has been developed that may limit procurement-related risks by assessing the performance of a candidate system in a simulated environment before it is chosen and implemented.

- **The National Military Research Project (NMRP), also known as Cyber Security Simulation Environment (CSSE)** for *reuse-oriented* Defence Network Model that supports modelling and simulation for Cyber Defence and tests on the effects of a cyber attack against command and control (**C2**) systems. As part of the efforts connected with the CSSE NMRP, we have analysed aspects and developments of Defence tools used in cyber warfare. *The Communication, Networking, and Cyber Modelling and Simulation Model* can effectively support Cyber Operations e Computer Network Operations scenarios by modeling and simulation of threats, vulnerabilities, and related countermeasures in a Cyber environment, and integrate real and simulated systems. In cyber warfare, supporting the creation of Cyber Ranges[1], Cyber Labs[2], Cyber Integration Test Beds[3] based on these tools may sustain Cyber Ops training and support. Also, it can foster the experimental development of concepts to acquire new capabilities as mentioned in the Joint Integrating Concept (012) (*Le attività militari nello spazio cibernetico. Cyber Warfare*, available in Italian). As far as concept development related to CN&C M&S, the following activities have been developed:

- **Unmanned Autonomous Systems (UAxS)**. These concepts have been defined to develop M&S architectures supporting experimentation to counter threats based on UAxS – e.g. robot swarms – with special focus on non-lethal aspects, such as using telecommunication networks for cyber activities.

- **Communication, Networking and Cyber Modelling and Simulation supporting Urban Operations**. A feasibility study for the modeling and simulation of a future city communication network based on the Archariae model was developed by the M&S CoE with a view to developing concepts and testing for Cyber Network Operations in future urban settings (Year 2035).

Based on our analysys, the Defence Communication, Networking and Cyber Modelling and Simulation capability rests on four aspects, namely reuse-oriented models, integration, interoperability, and performance. Finally, the Communication, Networking and Cyber Modelling and Simulation aspects dealt with in this paper support the evaluation of prospective application(s) and the implementation of such capability across Defence. As far as Cyber Defence in particular is concerned, the implementation of aspects such as reuse-oriented models, interoperability, integration, and performance would create an advantage for Defence in terms of return on invest-

[1] An infrastructure (range) based on real systems, networks, and visualisation techniques (virtual operational systems) employing on Human In The Loop to simulate attack and defence scenarios, study their effects, and deliver training.
[2] A laboratory that uses M&S tools to extend the capabilities of a Cyber Range in a limited environment.
[3] A laboratory (Battle Lab) where real and simulated systems are integrated with a view to concept development and testing in the cyber warfare domain.

ments for the activities being developed, and the current distribution of available and soon-to-be-available dedicated M&S tools.

3.2 Introduction

Innovations in Information and Communication Technology (ICT) have injected more and more technology in the military. Communication solutions have been adopted that are mandatory today to exchange information via telecommunication networks. Toghether with the evolution of military technologies, modeling and simulation has initially focused on force preparation and pre-deployment training vis-à-vis new operational scenarios, as well as on vehicle and equipment modernisation, and adaptation of training programmes. Nowadays, M&S' focus is on technology modernisation and implementation of the Defence net-centric concept, cyber defence, and UAxS. Communication, Networking and Cyber Modelling and Simulation is a technique that relies on models and simulations of technologies and communication networks whenever (i) replicating the behaviour of a real network as a complex system is required; (ii) complex network scenarios must be pictured and analysed in detail; and (iii) a technology or communication network model is required to conduct performance and simulation result analyses. The CN&C M&S aims at supporting the acquisition process of a complex system with due consideration to the system life cycle while using military technical requirements as a base. Through design, development, analysis, verification and validation tools for network architectures, the CN&C M&S can be used to depict and study information exchange. Also, cyber defence studies and analyses can be conducted to assess how telecommunication networks subject to cyber attacks react to different scenarios and what defensive measures should be adopted, which include both real and simulated systems, and how they interact, whereas autonomous systems can also play a role in either cyber attacks or defence. More specifically, this paper presents a CN&C M&S capability in support of the following:

- The *acquisition process*, by defining the technical aspects of the Technical and Operational Requirement (TOR) for the modernisation and rationalisation of the Defence Telecommunication Network;

- The analysis and evaluation of *cyber* scenarios by *using* the defence telecommunications network model again as part of cyber defence to test the effects of cyber attacks and the possible countermeasures;

- The development of concepts and testing concerning:

  - Unmanned Autonomous Systems (robot swarms);

  - Modelling of a future city telecommunication network to develop a live-virtual-constructive (LVC) simulation system.

3.2.1 Policy and Guidelines for Modeling and Simulation across Defence

*SMD-NEC001 — Modeling and Simulation Guidelines for the development of C4ISTAR Systems for Defence (**Linee di indirizzo di Modelling and Simulation per lo sviluppo dei sistemi C4ISTAR della Difesa**, [8] available in Italian only).* The net-centric transformation the Italian Defence intends to achieve requires defining its strategic implementation framework. The 6th Division of the Italian Defence General Staff supported by the Services Staffs, the Secretariat General of Defence, and the Joint Operational HQ – will draft the Modelling and Simulation Guidelines for the development of Defence C4ISTAR Systems. The national M&S guidelines will drive the effort to redress and otimise the capabilities of M&S Services Centres and the industry thanks to the four tasks of Simulation Centres, namely:

- Analysis and Acquisition for every operational mission/federation of systems (i.e. C4ISTAR), with the exception of CD&E;
- Analysis and Acquisition at sub-systems level;
- Field Training and Exercises;
- Operations Support.

The NEC-001 publication is currently under review at the Joint M&S Centre and the NATO M&S CoE in collaboration with the Centre for Defence Innovation (CDI). A Joint Integrated Capability (JIC) is also being developed under the title The Modeling and Simulation Capability Supporting Defence Transformation.

*SMD-NEC002 — 'Ministry of Defence Methodology and Architectural Framework to develop and define C4ISTAR and NEC Architectures' (**Metodologia e Framework Architetturale del Ministero della Difesa (MDAF) per lo sviluppo e la descrizione di architetture C4ISTAR e NEC**, [2] available in Italian only).* The aim of Directive SMD-NEC002 is the adoption of a standard methodology to analyse and define C4ISTAR and NEC architectures. This would support a standard transformation process to cope with specific operational requirements via efficient, consistent, and need-responsive solutions. The Ministry of Defence Architectural Framework (MDAF) is a framework-based methodology adopted by the Italian Ministry of Defence and included in Directive SMD-NEC002 as a reference to support design, analysis, and development of complex, net-centric C4ISTAR architectures. Adopting a standard model for the implementation of architectures represents a structured approach to managing complex architectures, and describing the possible views the architectures themselves offer. In order to develop the current methodological guidelines, Defence has adopted the NATO Architecture Framework (NAF) release 3.0, which represents the NATO framework for architecture definition and planning. Adopting NAF rel.3 as the archiectural framework of reference increases reusability of MDAF deliverables in multinational environments.

3.3 The Italian Defence TNN-NFON

The TNN is the radio-relay infrastructural network for the Defence and Services communication needs. The NFON is Defences wide-band fibre-optics communication network. Supporting the definition of technical requirements as well as drafting the Technical and Operational Requirement (TOR) within the acquisition programme for modernisation and rationalisation of the Defence TNN-NFON takes advantage of the CN&C M&S via modeling and simulation tools. With a view to choosing what technical solution to implement, an architectural model and the related TNN-NFON network model can therefore be created that define technical requirements, network performance analysis, and the Verification and Validation process . Choosing a methodology for the selection of M&S tools in support of acquisition and development of the TNN-NFON model relies on: (i) the directives and guidelines of the 6th Division, Defence General Staff Network Enabled Capability Series, SMD-NEC002 Directive '*Methodology and Architectural Framework of the Ministry of Defence (MDAF) to develop and define C4ISTAR and NEC Architectures*' (available in Italian only); (ii) the national NEC Force ITB, and (iii) the outcomes of several TNN and NFON workshops held over time to finalise the requirements. Using M&S tools means implementing the MDAF methodology and the related development tool for architectural frameworks called System Architect. This tool is required to design as-is and to-be TNN and NFON architectures to which modeling and simulation tools for telecommunication networks can be applied through the Riverbed Steel Central suite, formerly OPNET. The choice of the M&S tools required to model the TNN-NFON was based on the following four aspects:

- *Reuse-oriented models*. The network model created with Riverbed Steel Central suite can be used again for other projects or simulations. This applies, for example, to the required changes to network segments, network nodes, or to the inclusion of new network equipment. Concerning the possibility to reuse the model in other projects, a TNN model was developed for Sicily as a Proof of Concept (PoC) that can be extended to Italy as a whole. It was also applied to a NMRP called CSSE to test the behaviour of the network subject to a cyber attack; the effects on some national and NATO Command and Control systems have also been analysed.

- *Integration*. The network model can be integrated with a real-world network via a System In The Loop interface (SITL). Through integration, the simulated TNN network for Sicily obtained with the Riverbed Steel Central suite can be interfaced with real equipment, devices, and more via real protocols and achieve seamless exchange of data between the real and simulated domains;

- *Interoperability*. The Army, Navy, and Airforce use the respective network models generated as described above. Through the SITL module, these models interact with the network models of the other Services, i.e. all models of

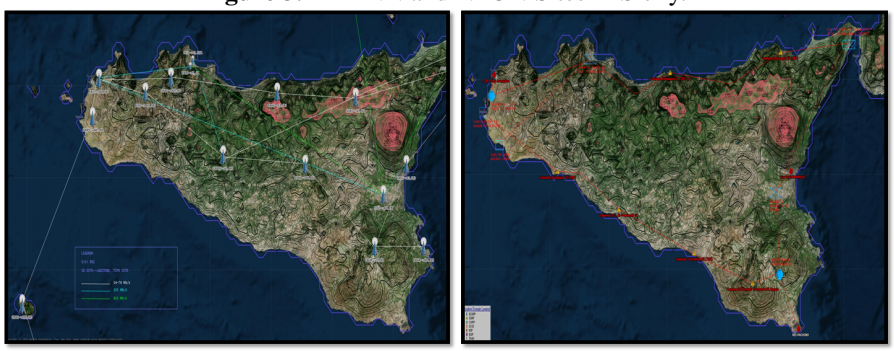
an entire network can interact with each other. Defence has invested in and provided the Services with a large number of Telecommunication Simulation and Evaluation environments based on Riverbed Steel Central suite to achieve interoperability of systems.

- *Performance*. Full IP network performance can be calculated through this model. With the adoption of a proper model in the future, Multi Protocol Label Switching (MPLS) will also be used to underpin design and technical choices. Performance will be measured based on the following variables:
  - End-to-end Quality of Service (QoS) and Quality of Experience (QoE) parameters;
  - Delay;
  - Jitter;
  - Packet loss ratio;
  - Traffic classes;
  - Network traffic routing;
  - Analysis of network traffic;
  - Line of Sight (LoS);

3.3.1 Modeling and Simulation Tools for Networks and Communication Systems

Modeling and Simulation of the TNN-NFON relies on the TSE modeling and simulation tool acquired by Defence. Through modeling, we can represent the major characteristics of the network as they emerge from the modernisation and rationalisation of TNN topology and its transition towards IP-based technology. This will initially apply to the PoC in Sicily and will be extended to the entire national network later by integrating TNN backbone and the IP-based NFON. As far as the migration of legacy TDM circuits to IP-based technology is concerned, modeling refocused analisys on Quality of Service (QoS) management as a pre-requisite for the migration of the TNN TDM-based IP traffic towards full IP traffic. In terms of topology, the network is a set of interconnected nodes, each node representing a JRR site linked to all others. Several meetings among experts have taken place and data collected to re-define the topology of the TNN backbone in the PoC in Sicily, including for the connection to the NFON IP sub-layer. Modeling and simulation of TNN and NFON the Defence General Staff Joint M&S Centre and the NATO M&S CoE have facilitated the analysis of data collected by the Services, the Joint C4 HQ, and the 6th Division of the Defence General Staff. Employing M&S tools has supported the creation of a TNN-NFON model where as-is TNN and NFON for the PoC in Sicily have been replicated and analysed. Future studies on performance will also

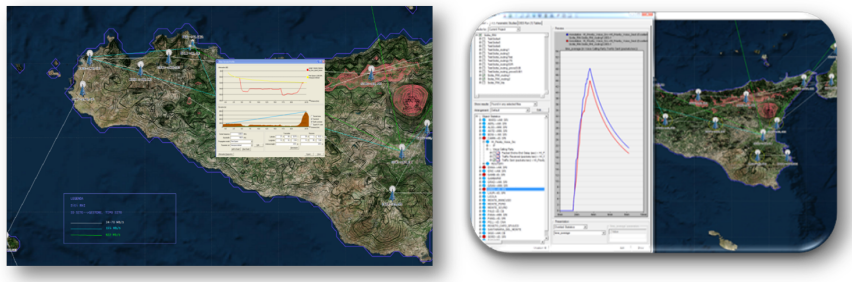
Figure 3.1 TNN and NFON Sites in Sicily.



be possible to proactively anticipate the required efforts and feasibility for the modernisation and rationalisation of such networks. The TNN-NFON model can be used to test performance whenever changes or upgrades to these networks are required. The initial TNN-NFON model focused on modeling, mapping, and georeferencing the current TNN and NFON nodes on national cartography. Initially, the ESRI ArcGIS software was used with data organised in Excel spreadsheets. Data referred in particular to the JRR sites (cfr. sheet labeled Infrastruttura), the users connected to the infrastructure (cfr. sheet labeled Utenti), and logical traffic across the network (cfr. sheet labeled Flussi). NATO M&S CoE staff has reorganised information in the spreadsheets, removed duplications and inactive sites, converted geographic coordinates from the sexagesimal scale (DMS) to the decimal scale (DEG), and uniformed general formatting so that each row of the Infrastruttura sheet matched a site and all its attributes. Later, the aforementioned native tool was used for modeling and simulation of the communications and networking components of telecommunication networks such as TNN and NFON. The tool can model and simulate whole eterogeneous networks characterised by wired and wireless technologies and all ISO/OSI layers, from physical to application. We have therefore managed to mirror the as-is TNN and NFON via esri ArcGIS on the TSE tool, which was used for analysis at a later stage. Figure 3.1 depicts the TNN (left) and NFON (right) models for the sites in Sicily. Through the tool and available data, the following deliverables were obtained:

- Modeling, mapping, and georeferencing of TNN and NFON sites on digital cartography;
- Analysis of elevation profiles among the different radio relay stations;
- Analysis of LOS versus terrain orography;
- Analysis of signal attenuation (dB) between radio relay stations;

Figure 3.2 Capabilities offered by the TSE M&S tool based on Riverbed Steel Central suite for the TNN.



- Measurement of distances between sites of the network;
- Detailed technical information for every site, which corresponds to a radio relay station;
- Modeling and simulation of VoIP (Voice over IP) traffic;
- Analysis of simulation results, notably end-to-end Quality of Service, packet delay, packet jitter, packet loss ratio, definition of traffic classes, routing of network traffic, analysis of network traffic, etc.;
- Possibility to connect the model with real systems via the SITL interface (this will be dealt with in details in the next section);
- 3D visualization:
  - by means of Preagis Stage and VegaPrime tools;
  - using the 3D Network Visualizer (3DNV) module, a native module of Riverbed Steel Central suite for which the M&S CoE has no licence, but can be supported by the Signals and ICT School;
  - on the web, via Google Earth.

Figure 3.2 contains a graphical representation of some of the capabilities the tool offers with respect to the TNN. In particular, the left picture shows the LOS analysis between two JRRs and the right image depicts the trend of the data packets exchange between the two JRRs versus time. Figure 3.3 shows the electromagnetic visibility test between the two JRRs of Antnennamare and Gambarie sites. The two sites are 32.77 kms apart. The elevation of the Antennamare site is 896.18 metres, while Gambaries is 1,320.85 metres, as shown in Figure 3.4. The graph shows the two sites have direct LOS (blue line), being the antennaes 20 metres high. The yellow ellissoid shown in Figure 3.5 represents the Fresnel zone. There are no obstacles

Figure 3.3 Electromagnetic Visibility Test.

Figure 3.4 LOS Test.

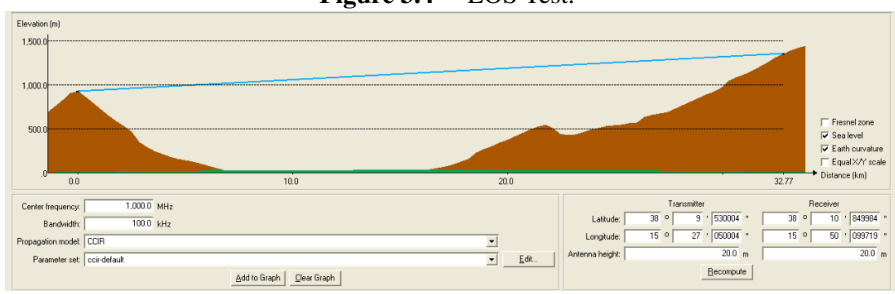
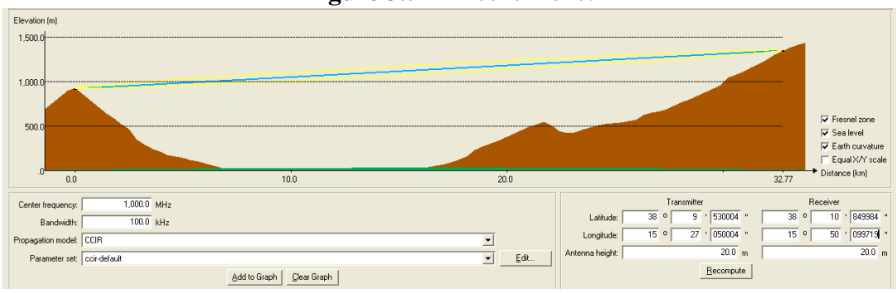


Figure 3.5 Fresnel zone.



intercepting the ellissoid and therefore no attenuation by diffraction exists for this link.

3.3.2 Communication, Networking and Cyber Modelling & Simulation Capabilities in support of Defence

Through the NEC Force programme, Defence has acquired M&S capabilities and established a federated network known as Integrated Test Bed (ITB) in a Basic Synthetic Environment (BSE) for each Service. Each of the ITBs is equipped with shared and ad hoc tools. Within the BSE, the Network Modelling and Simulation capability is available. The Signals and ICT School uses this capability at its best trough the Telecommunication Simulation and Evaluation Tool based on Riverbed Steel Central suite, the models customised for Defence needs, and the Government Off-The-Staff Joint Communication Simulation System (GOTS JCSS) of the US Defense Information Systems Agency (US DISA). Moreover, thanks to the CSSE NMRP (see details further on), the Signals and ICT School is acquiring a demonstrator model as an evolution of the TSE for the modeling and simulation of cyber attacks and related countermeasures within strategic and tactical military communication networks. As of February 2016, the Riverbed Steel Central licensing included in the Leonardo Telecommunication Simulation and Evaluation Tool of the NEC Force ITB sites is as in Table 3.1

The large number of licences available trhroughout Defence will allow other organisations to participate in modeling and simulation of the TNN-NFON project. Each Service will be responsible to model its own network as part of the national modeling effort. Defence will therefore obtain the best return on investments, especially for the possibility to use the whole TNN-NFON model again for the activities and goals each organisation has envisaged. This also applies to Cyber Defence through the Cyber ITB Battle Lab.

Table 3.1 Number of Riverbed Steel Central Licences in the ITB sites

NEC Force ITB	Number of Riverbed Steel Central (formerly OPNET) Licences
M&S CoE	1
Army Signals and ICT School ITB	4
Army Simulation and Unit Validation Centre ITB	1 + 1 BIT Phase 2 pending final test
Cavalry School ITB	1 — Pending final test
Infantry School ITB	1 — adequacy verification phase — pending delivery
Navy Programming Centre ITB	1
Navy Santarosa Compound ITB	1
Amendola Air Force Base ITB	1 — pending verification

3.3.3 Support to Procurement and Governance Model

Thanks to the analysis conducted by the NATO M&S CoE to support the implementation of the new TNN, the MDAF approach and the TSE-based simulation that supports procurement, TNN and NFON organisational and technical data will be acquired, managed, and presentated. In practical terms, a database for the development of the aforementioned networks can be created to correlate and aggregate both organisational data (capability nodes, operational nodes) and technical data (equipment, systems, characteristics, and standards). It can also be used to generate reports, while quickly accessing all essential information to define basic requirements for the future implementation of networks and final tests. Such data can be shown as reports for achitectural views, or in graphic form, with a view to a quick gap analysis between as-is and to-be models. With respect to as-is and to-be architectural models i.e. the Overarching Architecture (OA) and Baseline Architecture (BA) architectures considered when this paper was written, and the end-state architecture or rather the Reference Architecture (RA) and Target Architecture (TA) combined, respectively the data mentioned above can be used to build the network model and conduct simulations to measure network performance, manage QoS, analyse results, troubleshooting, verification and validation of simulation results and increase network performance. A detailed analysis of the major technical and operational characteristics of the sites to be created can be achieved through simulation, especially concerning migrations, so that prospective risk can be contained (simulate-before-you-buy). Last but not least and having reuse-oriented models in mind, these models can support the modeling of the MDAF C4ISTAR architecture and possibly offer a model of current TNN-NFON. Information available within the MDAF RA and TA architectural models delivered by the contractor and the implementation of the chosen solution will be the Baseline Architecture for the new architecture. The updated database

(Encyclopedia) will be implemented and used for future evolution, integration, and modernisation of TNN and NFON. As for the models delivered by the contractor, the integration via SITL interface with a real network enables design, testing, analysis, and verification and validation of new technological solutions via simulation, whose requirements can be detailed in TORs for future modernisation, development, and expansion efforts. Through reuse-oriented models, the status or the network can be monitored via network analysers and displayed. Simulation results concerning network performance trends obtained through the TSE tool can therefore be displayed in the network analyzer. A real time status will be available to present network faults and malfunctions, thus allowing operators to search for relevant causes. The network analysis tool may facilitate operators training, support performance analysis of the new network, and show the effects of cyber attacks. Based on the analyses and related options, the M&S CoE suggests the following governance model where the M&S CoE is:

- the Subject Matter Expert (SME), together with the Signals and ICT School, in the round table for drafting future TORs. These apply in particular to support modeling as-is NFON based on MDAF and modeling and simulation through TSE;
- the Joint Hub (cfr. ITB/NEC 001) for the federation of systems (SITL), i.e. the systems installed at the respective Services' ITB sites to ensure interoperability of simulation systems;
- the Subject Matter Expert (SME), together with the Signals and ICT School, to support Verification, Validation, and accreditation of models and architectures provided by the contractor;
- M&S CoE, together with the Signals and ICT School, will deliver M&S training for System Architect and TSE tools for modeling and simulation of TNN and NFON architectures.

Last, but not least, we suggest the Signals and ICT School should provide the Subject Matter Expert (SME) for simulation in cyber environments. Also, being the custodian for NEC Force TSE models already, the very School could also be the custodian for TSE-CSSE models.

3.4 Cyberspace. Cyber Security Simulation Environment: using the Defence TNN-NFON again

The Defence TNN-NFON telecommunication network model created by the M&S CoE has been used together with the models of a NMRP known as CSSE, where a number of **cyberspace** scenarios have been envisaged. The cyberspace is a cross cutting domain vis-à-vis the 4 traditional domains, namely land, maritime, air, and

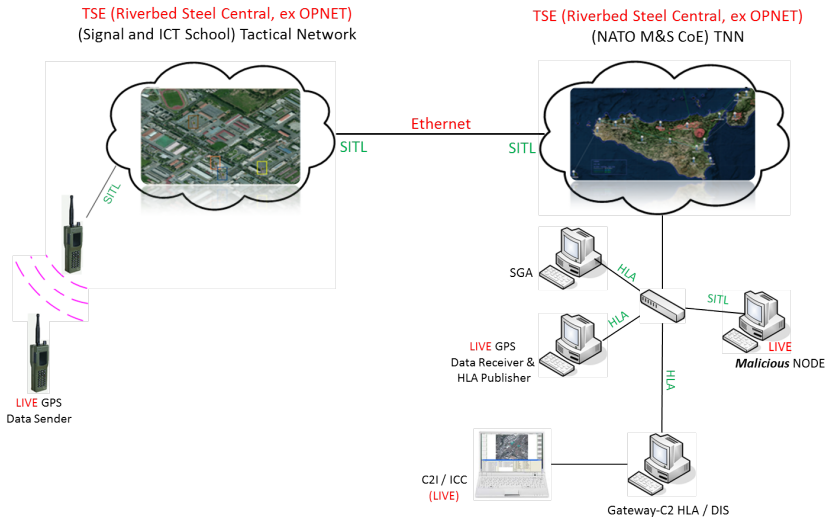
space. It is an artificial domain created the man has created and is characterised by interconnected telecommunications and computer systems. It has become an integral part to military operations and the information domain as a whole. The concept of **cyber attack** stems from the possibility that enemy forces take control of such domain. Cyber attacks should be considered as the "preliminary activities leading to the disruption of databases or information systems, cancellation or permanent alteration/manipulation of information contained therein." The implementation of cyber defence is therefore required as "a series of provisions, measures, procedures, and activities aimed at protecting (Defence) information systems and CIS infrastructures from hostile cyber actions in the widest sense. " Directive SMD-G-032 (2012) 'Policy in the Cyber Domain' and Law 124/2007 'Intelligence Organisation for the Security of the Republic and Secrecy' as amended by Law 133/2012 are the reference for approach Defence has chosen towards the cyber domain and to plan and conduct Computer Network Operations (CNO). With this in mind, **Cyber Modelling and Simulation** can support some kinds of Cyber Operations by modeling and simulation of different threats and vulnerabilities. The effects of attacks on ICT systems especially critical infrastructures based on Supervisory Control and Data Acquisition (SCADA) and the related defence techniques can therefore be analysed. The most common attacks against SCADA systems include planting Advanced Persistent Threats (APT) in the business network and reaching the connected SCADA network. Another form of attack consists in breaching the web-based interfaces for SCADA network management available on the Internet. Since the span of vulnerability is widening, security and protection solutions should be included in a model that protects data acquisition and access, communication system, and the technical infrastructures of the system itself. However, the lack of proper modeling and simulation tools to test the level of security of such systems is key. Applying CN&C M&S to cyber defence as a modeling and simulation technique for ICT systems and for the effects of cyber attacks on such systems may support cyber scenarios by modeling and simulation of threats, vulnerabilities, and countermeasures in offensive and defensive cyber environments and by integrating real and simulated systems. The CSSE project has been developed jointly by the Signals and ICT School, Leonardo-Finmeccanica (ETN Division - Innovation Lab), and the University of Catania, with the support of Joint M&S Centre, 6th Division, Defence General Staff, and the NATO M&S Centre of Excellence. It stems from the need to study cyber threats based on the growing importance of communications and the need to exchange sensitive information among units deployed in strategic and tactical scenarios. The project's main objective is to create an integrated simulation environment that includes operational scenarios, a span of possible threats, and the military communications networks with their equipment, communication protocols, and traffic to be analysed. Simulated cyber attacks can be brought against such scenarios to conduct dynamic testing and verify their response and the network resilience to the threaths. The M&S tool adopted as scenario generator and to reuse the TNN-NFON model is based on the Riverbed Steel Central suite, i.e. the most widely modeling and simulation tool for telecom-

munication networks used by both industries and universities. The CSSE uses a Live-Constructive solution to integrate live networks components in a constructive scenario. Tests and verifications can therefore be conducted quickly on real threats brought by live devices to simulated network architectures. Likewise, cyber attacks against real devices can also be tested. Figure 3.6 depicts the logic architecture of the CSSE PoC. A real radio network has been considered in the operational scenario made of two Army-issued HandHeld Software Defined Radios (SDR HH). Live GPS data are sent to another real radio connected to the tactical network model via SITL interface created on the TSE tool at the Signals and ICT School. The link between the real world (military radios) and simulated world (tactical network) is therefore self-evident. The tactical network model is superimposed over the map where real radios are represented and the position of other simulated radios is displayed together with the real radio sending GPS data. GPS positioning data sent by the real radio via the simulated tactical network travel across the simulated Defence TNN to a command post hypotetically located in Sicily and displayed on the C2I/ICC command and control systems, which are also simulated. This represents a full two-way interaction between the simulated world and the real world (C2 systems). Thanks to the HLA federation, the simulated TNN is connected to other systems, such as the Scenario Generator Animator (SGA) for the logistic management of simulated items, the LIVE GPS Data Receiver and the HLA Publisher. Through the latter, positioning data are sent by the LIVE GPS Data Sender and the C2-Gateway — which translates geopositioning data in a format readable by C2 systems — across the federation. The LIVE Malicious NODE, as the name suggests, is a real system connected to the federation and represents the logical node generating the cyber attack. More specifically, when the attack is unleashed, the LIVE Malicious NODE steals the identity of the LIVE GPS Data Sender and injects false positioning information into the federation. The LIVE GPS Data Receiver & HLA Publisher will itself publish false geographical information for the LIVE GPS Data Sender. As a result of the cyber attack against the real radio, the C2 systems will read a fake position for the Live GPS Data Sender radio. Eventually, once the attack has ceased, the C2 systems will display the real position of a LIVE GPS Data Sender radio.

The CSSE demonstrator tests the network functionalities during and after a cyber attack, together with the effects on NATO and national command and control systems. The available CSSE demonstrator is an open and unclassified environment to indipendently test cyber threats affecting tactical networks and, more in general, telecommunication networks. Based on previous considerations, the entire national model of TNN-NFON can be used again in a cyber environment to test possible attacks against tactical and physical networks and therefore to identify countermeasures or analyse the effects of attack methodologies or national defence techniques. Cyber Modelling and Simulation can support Cyber Lab activities through:

- modeling and simulation of new cyber security techniques;
- verification and validation of defensive tools;

Figure 3.6 Cyber Attack Scenario.



- exercises and training for cyber defence personnel;
- design and development of tactics, techniques, and strategies to counter threats;
- a simulation environment for Unmanned Autonomous Systems known as UaxS Cyberspace Arena (UCA)

3.5 Unmanned Autonomous Systems

To date, there is no shared definition of autonomy from a technical standpoint, except for independence of software as the defining character of future and autonomous machines. These will alter the current tactical and operational scenarios provided some mandatory parameters are defined for such increasingly unmanned machines, including reliability, cost-effectiveness, integration, and interoperability. The NATO M&S CoE provides support to NATO ACT for concept development and experimentation concerning Unmanned Autonomous Systems (UAxS) [3,5]. In this paper, all the autonomous/smart systems deployed in tactical and operational naval, air, or land scenarios, e.g., current drones and UAVs, are considered Unmanned Autonomous Systems (UAxS). Given their constant development and increased use in tactical scenarios, such drones — and especially the communication infrastructure these systems rely on exchange data — are vulnerable to cyber threats. Therefore, the CN&C M&S capability can also be applied to UAxS. Our main objective is to develop a simulation environment called UAxS Cyberspace Arena (UCA) [4] to realize

a communication infrastructure among UAxS that is able to implement countermeasures in case of a cyber attack against such infrastructure. The arena is inspired by the Cyber Range and Cyber Lab concept. The UCA is based on the implementation of an integrated simulation environment where the UAxS tactical telecommunication network can be evaluated and tested, the threats posed against UAxS' scope of action, and the relisience of such systems to security systems. Once implemented, the architecture and simulation environment can be used during the experimentation phase of the Joint Concept Note for autonomous systems conducted by the Centre for Defence Innovation and used again to develop cyber range(s)-related concepts.

3.6 Urbanisation Project, Archariae Model and Simulation of Communication Networks

The Urbanisation Project was commissioned by NATO SACT to the NATO M&S Centre of Excellence and focuses on the creation of a 2D/3D model of a future city to evaluate the effects of city disorders, impact of mass migrations, and effects of natural disasters. The objective is a prospective 2035 city spanning over 1,700 sq kms and having a population of 5 millions. The city is built by superimposing layers as shown in Figure 3.7. Every layer represents one of the essential elements of the city, e.g. the transportation network layer, the electrical grid layer, the water grid layer, and so on. Communication, Networking and Cyber Modelling and Simulation also applies to this environment. More specifically, a model of the telecommunication network has been created to include land and mobile communications, Sat TV, and radio broadcasting via FM antennaes. The land and mobile network was the first to appear in the architecture model.

The model of telecommunication network follows a tree architecture as shown in Figure 3.8. The Transitional Switch represents the root and the network entry point connected to the regional switches that serve the area under consideration. Every Regional Switch is linked to Local Switches representing the terminal points for the network architecture, i.e. the switches delivering the land network service. As far as the mobile network is concerned, another architectural layer has been added so that every Local Switch is logically linked to a Base Radio Station, also known as Base Station or Tower, whose coverage is typically depicted as a hexagonal-shaped cell. The base station represents the connectivity hub for mobile devices — namely smartphones, laptops, and tablets — within the base station coverage. Every cell can support up to 200 mobile users. The telecommunication network architecture model for the Urbanisation Project has been implemented using the esri Geographic Information System (GIS) tool. Figure 3.9 shows the model for the land network. The distribution of the network architecture's Transactional Switches, Regional Switches, and Local Switches is also clearly visible. Figure 3.10 shows the model for the mobile network and the base radio stations, with their polygonal area around every radio station. Within every area, or cell, coverage can be calculated with special algory-

Figure 3.7 Urbanisation Project Layer.

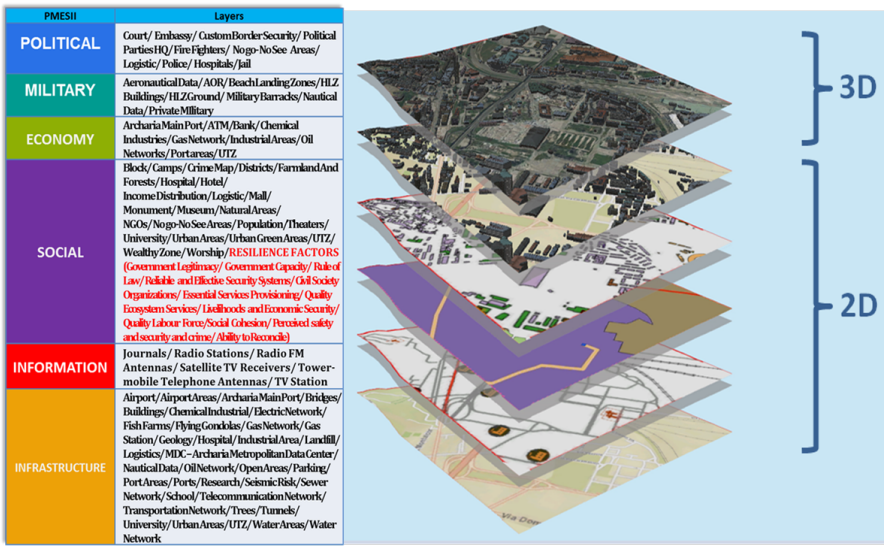


Figure 3.8 Urbanisation Project Telecommunication Network Scheme.

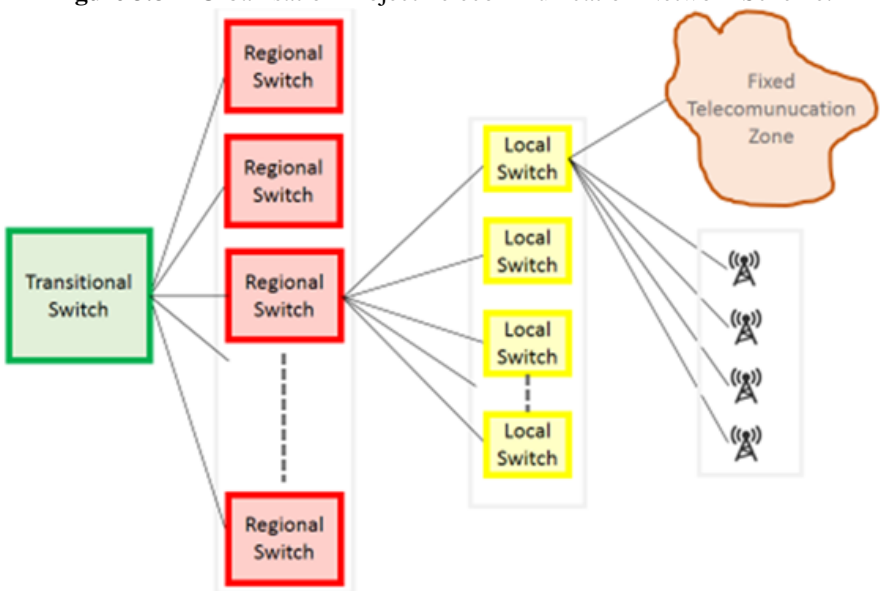


Figure 3.9 Land Network Model.

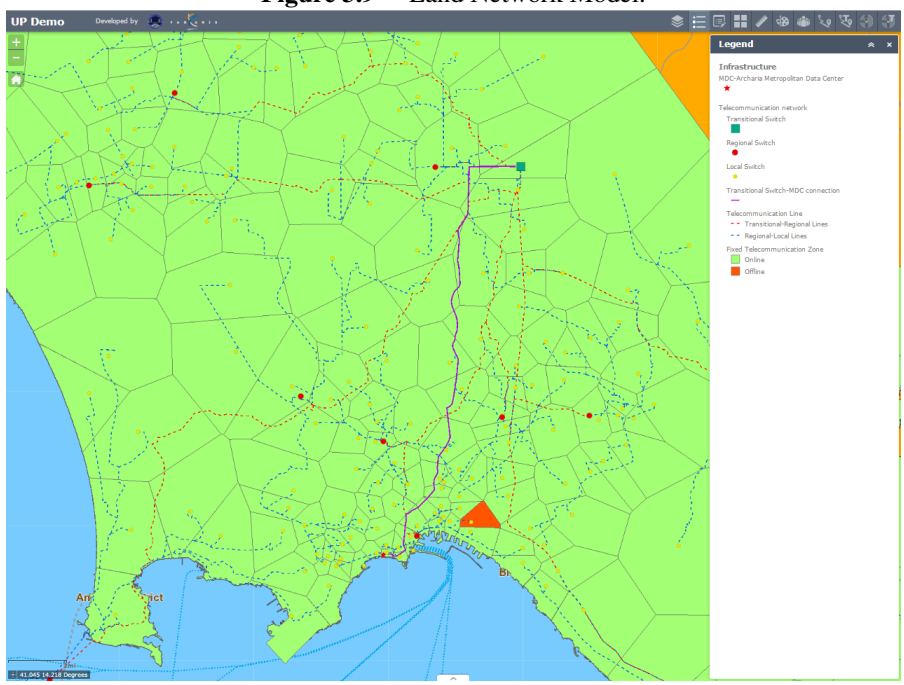
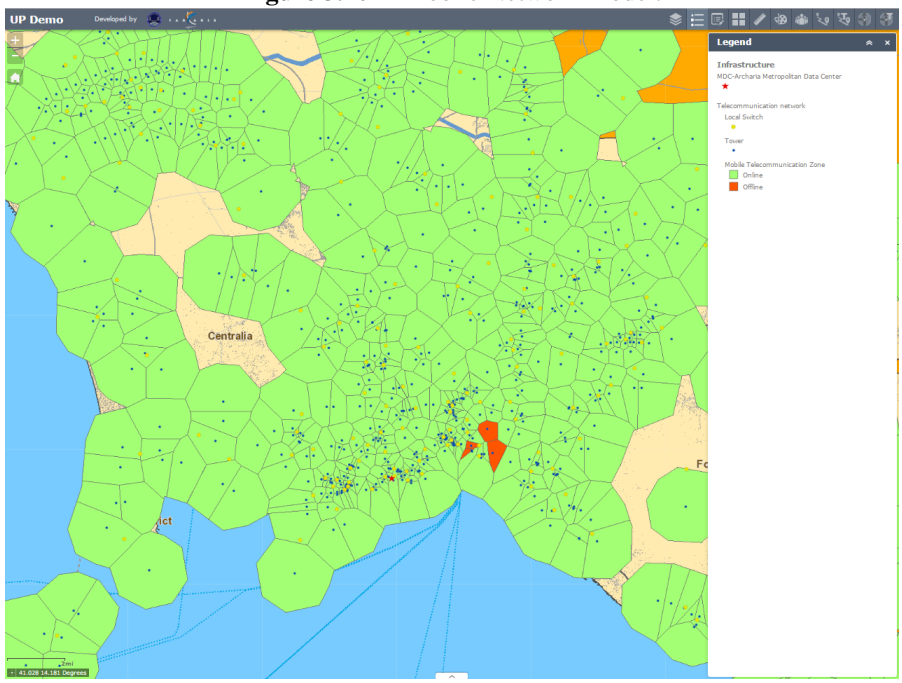


Figure 3.10 Mobile Network Model.



thms included in the esri tool, so that users present in every cell of the mobile network can be provided mobile connectivity. The area depicted in orange shows a service outage. The impossibility to provide telecommunication services can be attributed to one of the aforementioned three reasons, namely:

- City disorders;
- mass migrations, and
- effects of natural disasters.

In the first phase of the Urbanisation Project, a static model called Archaria was created to reflect a model of the telecommunication network infrastructure. Through TSE M&S tools, the Archariae model telecommunications can be simulated, with a view to modeling and simulation of all aspects of the mobile network. Its performance under normal conditions, or in case of city disorders, mass migrations, or natural disasters can therefore be measured. Thanks to the tool, the effects of M&S of data exchange across the Archariae model telecommunication network's Unmanned Autonomous Systems could also be measured, and the employment of C2 and Decision Support Tool evaluated together with the effects of possible cyber

attacks. This is consistent with the ideas presented above about the cyber domain and ensures redeployment for military networks, and support to the planning and rehersal phases.

3.7 Conclusions

This paper shows how modeling and simulation applications have become key and unavoidable elements of support to several military activities, including with reference to telecommunications and cyber domains. In particular, this refers to using M&S to support the acquisition process during the drafting phase of the Technical and Operational Requirement for modernisation and optimisation of the TNN-NFON, or in cyber space for the modeling and simulation of events that may alter the normal functioning of network infrastructures for information exchange — also known as Cyber Security Simulation Environment —, or whenever the employment of Unmanned Autonomous Systems (UAxS) is envisaged in cyber scenarios. Last, but not least, how CN&C M&S can support telecommunications modeling in *urban environments* is presented, together with the *effects on military operations*. All these activities show that *reuse-oriented models*, *integration*, and *interoperability* at the joint level go hand in hand with the dedicated M&S tools available on the ITB sites of Services. Reuse-oriented models, interoperability, integration and performance earn Defence an advantage in terms of return on investments, given the number of Riverbed Steel Central (former OPNET) licenses on which the TSE relies that have been purchased and distributed across Defence. Starting from the ideas of integration and interoperability as related with the TNN-NFON project, the modeling and simulation efforts for national networks can be broken down and assigned to ITBs so that every Service takes care of modeling and simulation for the respective network and aspects of interest. Finally, the Communication, Networking and Cyber Modelling and Simulation aspects dealt with in this document support the evaluation of possible applications and use of these capabilities across Defence. This refers in particular to cyber defence, the development of cyber labs, and to training and specialisation of personnel who will be employed in the Communication, Networking and Cyber Modelling and Simulation sector.

REFERENCES

1. Stato Maggiore della Difesa, VI Reparto Sistemi C4I e Trasformazione, ”SMD–NEC–001 Linee di indirizzo di Modelling & Simulation per lo sviluppo dei Sistemi C4ISTAR della Difesa”, Rome, Italy, IDGS document, (2007).

2. Stato Maggiore della Difesa, VI Reparto Sistemi C4I e Trasformazione, ”SMD–NEC–002 Metodologia e Framework Architetturale del Ministero della

Difesa (MDAF) per lo sviluppo e la descrizione di architetture C4ISTAR e NEC ", Rome, Italy, IDGS document, (2009).

3. M. Biagini and F. Corona, "Modelling & Simulation Architecture Supporting NATO Counter Unmanned Autonomous Systems Concept Development", *Third International Workshop, MESAS 2016, LNCS 991*, pp. 118-127, Springer International Publishing, J.Hodicky (Ed.), (2016).
4. M. Biagini, S. Forconi, F. Corona, A. Mursia, L. Ganga and F. Battiati, "The Unmanned Autonomous Systems Cyber Arena (UCA). A M&S Architecture and Relevant Tools for Security Issues Analysis for Autonomous System Networks", *Third International Workshop, MESAS 2016, LNCS 991*, pp. 168-175, Springer International Publishing, J.Hodicky (Ed.), (2016).
5. M. Biagini, A. Scaccianoce, F. Corona, S. Forconi, F. Byrum, O. Fowler and J. L. Sidoran, "Modelling and Simulation supporting unmanned autonomous systems (UAxS) concept development and experimentation", *Proceedings of Disruptive Technologies in Sensors and Sensor Systems (SPIE Defense and Security)*, vol. 10206, Anaheim, CA (USA), (2017).

CHAPTER 4

NATO MSAAS – A COMPREHENSIVE APPROACH FOR MILITARY OPERATIONAL REQUIREMENTS DEVELOPMENT

Marco Biagini, Michele La Grotta, Fabio Corona, Sonia Forconi[1], Marco Picollo and Christian Faillace[2]

[1]M&S Centre of Excellence, Rome, Italy
[2]Leonardo, Land & Naval Defence Electronics Div., Genova, Italy

This paper originally appeared in the 2016 Proceedings of the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC)

4.1 Introduction

To a great extent, and according to the NATO M&S masterplan "NMSMP" [1], future military capabilities (i.e., doctrine, training, operations, etc.) will be developed and supported by Modelling and Simulation (M&S). Two main barriers are cost and accessibility. M&S technology is highly valuable to NATO and military organizations. To underline the importance of M&S in NATO, the North Atlantic Council (NAC) set up the NATO Modelling and Simulation Group (NMSG) to supervise the implementation of the NMSMP and to propose updates, promoting co-operation among Alliance bodies, NATO member nations and partner nations to maximize the effective utilization of M&S [2]. According to this vision, it is essential that M&S tools are conveniently accessible to a large number of users as often as possible. To achieve a so widespread accessibility a new M&S framework is required, where M&S tools can be accessed simultaneously and spontaneously by a large number of users for their individual purposes. This "as a Service" paradigm has to support stand-alone use as well as integration of multiple simulated and real systems into a unified simulation environment whenever the need arises.

The NATO Modelling and Simulation Group MSG-136 ”Modelling and Simulation (M&S) as a Service (MSaaS)” has defined MSaaS as ”the combination of service-based approaches with ideas taken from cloud computing” [3] . MSaaS seems to be a promising approach for realizing next generation simulation environments. This group was tasked to investigate, propose and evaluate standards, agreements, architectures, implementations, and cost-benefit analysis for incremental implementation of a permanently available, flexible, on-demand cloud-based services framework to provide M&S tools on-demand accessible to a large number of users. Furthermore, the NATO M&S Centre of Excellence (CoE) in collaboration with Leonardo Finmeccanica are contributing to the NMSG 136 working group in the design of an experimentation environment to support MSaaS experiments known as the Open Simlab initiative.

4.2 NATO CD&E approach to MSaaS operational Concept Development

Concept Development and Experimentation (CD&E) for NATO is an enabler for transformation through the structured development of creative and innovative ideas into viable solutions for capability development. Paraphrasing the NATO CD&E Policy [4], Concept Development is a process aimed at finding solution-oriented transformational ideas that address capability shortfalls or gaps. The development of the MSaaS concept is of this kind, in which NATO would like to take advantage of new technology to obtain new capabilities.

4.2.1 NATO Capability Development Comprehensive Approach applied to MSaaS

In the NATO framework, a capability is a ”the ability to execute a specified course of action or achieve a certain effect” and when it is necessary to introduce a new capability several aspects should be taken into account, adopting the so called ”comprehensive approach”. Different components could need changes or completely new developments. The components that are considered are: Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability (DOTMLPFI). In details, the meaning of each component, as from NATO CD&E Handbook is adapted in the following, the Allied Framework for M&S as a Service as defined by the Operational Concept Document (OCD) Draft [5] under development by the MSaaS OPS Sub groups analysed using the DOTMLPFI approach.

- **Doctrine** (*The way we use MSaaS to support capabilities development*): MSaaS is considered a modernization of existing M&S capability and technology. Although major doctrine changes are not expected, minor revisions or adaptations may be required.

- **Organization and Policy** (*How to organize NATO and Allied M&S structures*): The need for an Allied Framework for M&S as a Service results from national policies like the UKs Defense ICT Strategy [6], US DoD Cloud Computing Policy [7], the ITA MoD NEC001 [8] and NATO policies [9]. Establishing the Allied Framework for M&S as a Service requires installation of an MSaaS Governance Authority (as defined by Allied M&S Publication AMSP-02 / Standardization Recommendation, STANREC 4794) and accompanying policies (e.g., mandating the sharing of M&S resources). Establishment of national and/or NATO "Simulation Centres" that have oversight of national/NATO MSaaS activities. Adopting the Allied Framework for M&S as a Service will influence procurement as M&S services may be acquired on a pay-per-use or share-principle and ownership is not necessarily transferred. This has impacts on the relationship of provider (e.g., industry) and buying authorities.

- **Training** (*How we prepare NATO and Allied MSaaS specialists*): Training is required to prepare users (e.g. Exercise Control (EXCON)/Simulation Control (SIMCON) staff) to fully utilize the Allied Framework for M&S as a Service (e.g., to discover simulation services, to orchestrate and deploy services, etc.). MSaaS should enable and transform training in NATO, improving quality and quantity [10]. MSaaS will require new skills (e.g., regarding cloud computing, virtualization, service-oriented architectures, and emerging M&S-related technology etc.) and appropriate education and training.

- **Leadership** (*Chain of Command and Control and relationships in NATO and Allied according to MSaaS*): To realize the full potential of MSaaS, an enterprise approach is required which requires senior leaders to approve the MSaaS concept and to support the transformation activities.

- **Materiels** (*All the hardware, software, equipment and systems related to MSaaS necessary to NATO and Allies to manage, to support and to develop M&S Services*): The MSaaS concept requires establishment of a cloud infrastructure and appropriate network connections/infrastructure. Full adoption of MSaaS requires gradual transformation of existing M&S applications, data, etc. to comply with the MSaaS concept.

- **Personnel** (*Availability of qualified people according to MSaaS needs*): It is expected that the amount of resources required for preparing and conducting exercises and experimentation are reduced (less personnel to run EXCON/SIMCON, less administration efforts due to automation, etc.). It will likely be required to educate/re-skill personnel.

- **Facilities** (*Data Centres, Training facilities and Battle Labs available to provide and to consume MSaaS services*): Cloud infrastructure and appropriate data centres are required.

- **Interoperability** (*How to provide interoperable and accessible MSaaS services in NATO and Allied Overarching MSaaS Architectures*): The MSaaS concept promotes an open systems approach and requires the adoption of open standards (for data formats, protocols, etc.). If required, existing proprietary solutions need to be replaced by open standards. To enable the MSaaS concept, sharing of M&S resources needs to be mandated.

4.2.2 MSaaS Conceptual Architecture Development

The MSaaS architecture development is based on a standard methodology called NATO Architectural Framework (NAF) [11] based on the TOGAF(TM) Architecture Development Method (ADM) [12] with input from other sources such as the MODAF (The UK Ministry of Defence Architecture Framework) learning portal and systems engineering standards, such as ISO15288 [13]. The NATO Architecture Framework (NAF) is an Enterprise Architecture (EA) framework by NATO. The Enterprise Architecture provide decision support, in the context of the enterprise strategy, for the use of resources (processes and procedures) in the enterprise. The architecture is responsible for defining how resources (M&S services) will be used to support enterprise strategy (MSaaS implementation plan) and benefit the NATO goals and objectives as defined by the MSaaS Operational Concept according to the NATO M&S Masterplan.

4.3 MSaaS Activities

4.3.1 NATO Modelling and Simulation Group

The NATO Modelling and Simulation Group (NMSG) is conducting activities related to the MSaaS concept development and experimentation. The preliminary study was performed by the MSG-131 specialist group with the follow-on activity MSG-136. This section will introduce briefly these activities.

4.3.2 NMSG 131 Technical Report

According to the results of the NATO MSG-131 [14], a main conclusion of the specialist team is that service-based approaches to M&S offer many potential benefits, taking advantage of recent technical developments in the area of cloud computing technology and Service Oriented Architectures (SOA). Moreover, an alignment of ”M&S as a Service” with the Connected Forces Initiative (CFI) is required, as the primary objective of the CFI (i.e., sharing and pooling of resources) is resembled in MSaaS. Similarly, it is required to align M&S and MSaaS with the NATO Consultation, Command and Control (C3) Classification Taxonomy as this is the primary tool used by NATO to chart the NATO C3 landscape. The general approach taken

by this specialist team was to perform a survey of the experiences from members regarding the use of cloud computing and service-oriented approaches within the M&S domain. The goal was to agree upon a shared understanding of what "M&S as a Service" is within NATO and to provide a comprehensive documentation of MSaaS case studies with an overview of existing service-oriented architectures in the M&S domain. Based on these existing experiences and architectures, conclusions and recommendations derived on the way forward. The following definition of MSaaS derived from the "service" definitions provided by ITIL glossary [15] and ISO/IEC 20000 [16]: *"M&S as a Service (MSaaS) is a means of delivering value to customers to enable or support modelling and simulation (M&S) user applications and capabilities as well as to provide associated data on demand without the ownership of specific costs and risks."* Several perspectives of the MSaaS concept arising from this definition, as follows:

1. MSaaS as a cloud service model;
2. MSaaS using cloud service models;
3. MSaaS as a Service Oriented Architecture;
4. MSaaS as a business model.

The hands-on experiences with the identified case studies (15) provided guidance and candidates for architectures, data models and interfaces that could become future SISO standards. In accordance with its Technical Activity Description, MSG-131 recommended to investigate MSaaS in more detail.

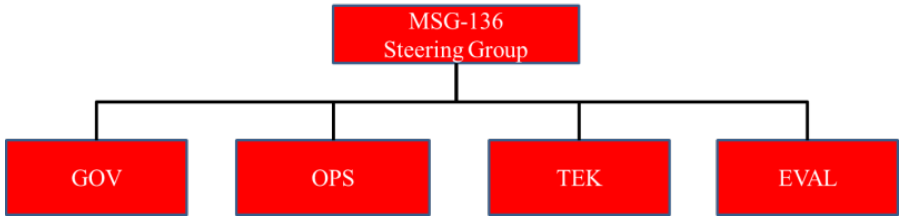
4.3.3 NMSG 136 Activities

The "MSaaS: Rapid deployment of interoperable and credible simulation environments" (NMSG-136) is the Science & Technology Organization (STO) research task group which received the heritage of MSG-131. Its objectives are to investigate, propose and evaluate standards, agreements, architectures, implementations, and cost-benefit analysis of the MSaaS approach. Specifically, with regards to evaluation of the use of M&S domain services to improve simulation interoperability and credibility, and to the analysis of the organizational M&S services perspective to establish a sustainable and efficient management of M&S services in NATO. The MSG-136 is composed by several sub-groups as illustrated in Figure 4.1.

In particular, the goals and expected deliverables of each sub-group are here detailed:

- Governance (GOV) Sub-group: defines policies for joining the MSaaS Ecosystem and defines how to maintain MSaaS Ecosystem. Its main deliverable is the AMSP-02, which contains these policies and standards;

Figure 4.1 MSG-136 organization.



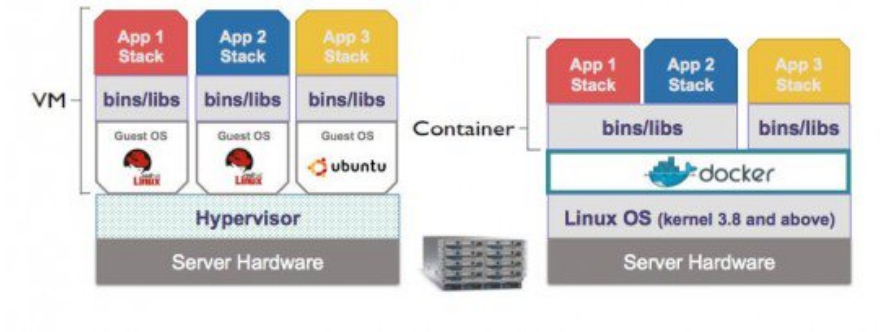
- Operations (OPS) Sub-group: develops operational concepts and describes the desired characteristics and requirements of the MSaaS Eco-System from a users perspective, including its major structures and capabilities to create an MSaaS Reference Architecture (RA). Its main deliverable is the Operational Concept Document (OCD);
- Technical Perspective (TEK) Sub-group: conducts technical investigations and experiments using specific MSaaS Target Architecture aspects to help generate MSaaS Reference Architecture, detailing the technical requirements for M&S Services using the MSaaS Target Architecture. Among its deliverables can be found the Technical Reference Architecture, the Service Description Template, the NATO Architecture Framework (NAF) descriptions and the Reference Engineering Process;
- Evaluation (EVAL) Sub-group: explores opportunities to participate in experimentation venues to test some implementations of the MSaaS RA, e.g., test beds with a Target Architecture derived from the RA.

In this context, the M&S CoE and its industrial partners are participating in the development of the MSG-136 deliverables and they are building a first experimental cloud infrastructure to conduct experimentation on the MSaaS concept. Moreover, the M&S CoE was leading the EVAL sub-group, which participated in the 2016 edition of the Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX), as part of the M&S Focus Area, under the coordination of the same M&S CoE.

4.3.4 CWIX

The NATO CWIX programme provides a unique venue that allows systems and network engineers to come together to solve existing interoperability issues and explore and share potential solutions in anticipation of future operations and budget constraints, an opportunity for NATO commands/agencies and member and partner nations to prove, disprove, and improve NATO, National and Coalition Communication and Information Systems Interoperability. During this event, initial MSaaS ex-

Figure 4.2 VM vs Container technology.



perimentation was performed. In particular, via the unclassified network of the Joint Training Force Centre (JTFC), a Scenario Generator and Animator (SGA) acted both as consumer of services generating scenarios and as provider of services through a Computer Generated Forces (CGF) service. In addition, other capabilities where provided under a service paradigm, like the United States Air Tasking Order Generator (ATOG), which generated flight tracks from Air Task Orders (ATOs).

4.4 MSaaS Technology — State of the Art

4.4.1 Cloud technology and Containers solution

Cloud computing, often referred to as simply ”the cloud”, is the delivery of on-demand computing resources over the Internet on a pay-for-use basis or in a private environment [17]. The main enabling technology for cloud computing is virtualization. Virtualization software separates a physical computing device into one or more ”virtual” devices, each of which can be easily used and managed (Virtual Machines) to perform computing tasks. This technology minimizes user involvement, provides automation to speed up the process, reduces labor costs, and reduces the possibility of human errors. Cloud computing provides all of its resources as services, and makes use of the well-established standards and best practices gained in the domain of SOA to allow global and easy access to cloud services in a standardized way. Today another kind of virtualization is available, operating-system or kernel-virtualization called Containers Virtualization. With operating-system-level virtualization essentially creating a scalable system of multiple independent computing devices, idle computing resources can be allocated and used more efficiently. (Figure 4.2)

This technology adds a new layer to cloud-computing; so the layers accessible within a stack are now IaaS (Infrastructure as a Service), PaaS (Platform as a Ser-

vice), SaaS (Software as a Service) and CaaS (Container as a Service). IaaS refers to online services that abstract the user from the details of infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc. A hypervisor, such as KVM and Xen, VMware ESX/ESXi [18], or Hyper-V [19] runs the virtual machines as guests. PaaS vendors offer a development environment to application developers. The provider typically develops toolkit and standards for development and channels for distribution and payment. In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming-language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. Conversely, in the SaaS model, users gain access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as ”on-demand software” and is usually priced on a pay-per-use basis or using a subscription fee. In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. CaaS is a type of IaaS, such as a Docker (an open platform to build, ship and run distributed applications), specifically geared toward efficiently running a single application. A container is a form of operating system virtualization that is more efficient than typical hardware virtualization. It provides the necessary computing resources to run an application as if it is the only application running in the operating system – in other words, with a guarantee of no conflicts with other application containers running on the same machine [20].

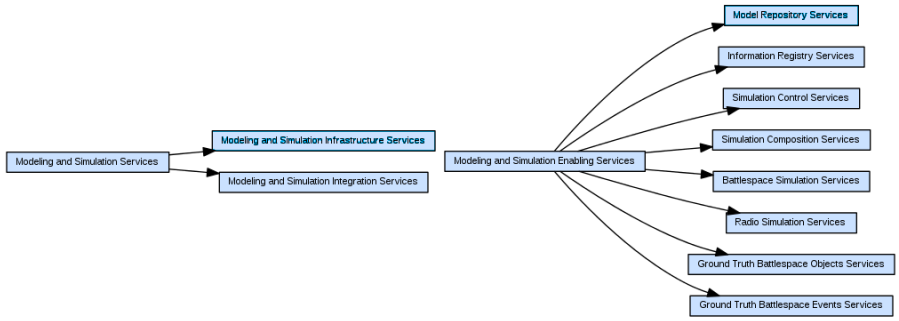
4.4.2 Cloud Security

Common security challenges for cloud services are listed as the top security threats to cloud computing by the Cloud Security Alliance (CSA). In addition to the twelve most treacherous threats, considering an international Military MSaaS environment and its architectures, another major challenge is the so called multi-level security (MLS). Benefits of an MSaaS can be fully achieved when true multi level security (MLS) is realized. That means all users with different clearances can access a cloud, and an automated security mechanism can guarantee secure flow control and sanitization [21].

4.5 MSaaS Enterprise Architecture

The Open SimLab initiative by the NATO M&S CoE consists of an innovative business model developed to attract industry, academia and organizations (NATO, military/governative/non-governative agencies) based upon the use of M&S in or-

Figure 4.3 C3 Taxonomy — M&S COI Services.



der to experiment on new concepts and ideas involving the integration of different systems and technologies.

4.5.1 The Open Cloud Ecosystem ApplicatioN (OCEAN)

The OCEAN project is being developed by the Leonardo Company under a technical agreement with the NATO M&S CoE. To develop the project further other partners are joining the NATO M&S CoE under the Open Simlab initiative. The aim of OCEAN is to provide to MSaaS Community of Interest (CoI) and other partners an experimentation environment based on cloud technology. In this embryonic framework, it is possible to consume the available MSaaS services, and/or deploy new M&S services, for testing and experimentation purposes to verify and exploit the MSaaS operational concept development. A set of fundamental Modelling and Simulation services are categorized under the C3 Taxonomy as COI-Specific and COI-Enabling services [22] (NATO ACT, 2012, June 15) (see Figure 4.3):

The following basic services are available in the cloud infrastructure provided by the OCEAN prototype:

- Infrastructure/Integration Services: allows users to interconnect each other, from Voice over Internet Protocol (VoIP) to VTC to specific M&S applications, such as High Level Architecture (HLA) Run Time Infrastructure;

- Synchronization Services: allowing systems being time-synchronized especially useful for real-time applications, mainly based on Network Time Protocol;

- Information Exchange Gateways Services: useful whenever a connection between systems using different interfaces is necessary; they can translate the exchanged information inside the simulation network or between simulation and real systems;

- Information Registry and Model Repository Services: allows users to get information about the available services and assets and to have access to a repository of models;
- Simulation Composition and Control Services: assembles the necessary components together to control the overall execution of the experiment;
- Terrain Databases and geospatial Services: shares terrain data information and guarantees coherence and proper correlation among all of the participants;
- Synthetic Scenario (Battlespace) Services: a widely used set of services to generate and animate a shared virtual reproduction of a real-world situation, in terms of static and moving entities and their interactions;
- Communication Services: used whenever a simulation of real-world radio or network communications among entities and systems is necessary.

4.6 MSaaS Framework

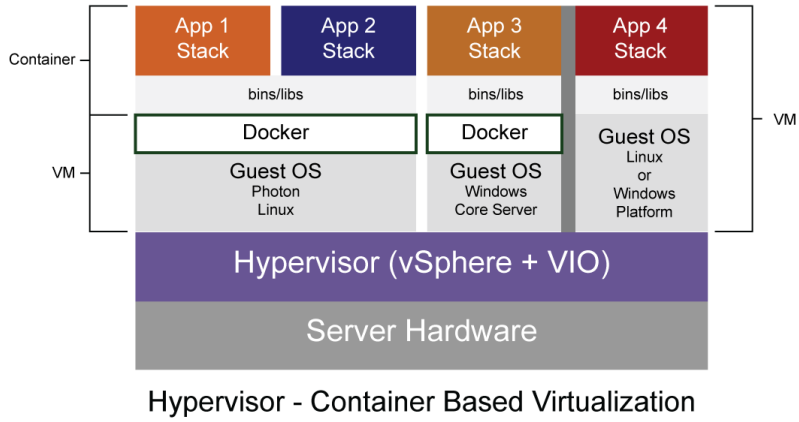
The OCEAN project offers an embryonic framework made of a combination of hardware, software and services (”platform as a service”, ”software as a service”, ”data as a service”) to automate the deployment of M&S tools and applications in a cloud environment. The framework offers a unique point of access through a web portal. The web portal provides a secure environment with access to the portal resources (services) granted by a user identity management system. The availability of services is managed by an M&S services management system, who facilitate the delivery, versioning, testing, consumption, termination and disposal of services. The main phases of the services management are identified as follows:

- Services Provisioning: preparation of the available services
- Services Deployment: making the services available to users through the cloud system
- Network Provisioning: automating network reconfiguration
- Services On-demand: users services consumption

The above phases can be performed through the following sessions:

1. Sessions isolation: Test, experimentation, integration and training sessions are virtual separated environments (sessions) inside a cloud. The session isolation allows a multi-tenant services consumption by users, partitioning service applications with one or more customized virtual instances that are independent from each other in the cloud.

Figure 4.4 Hypervisor and Container-Based Virtualization Services.



2. Integration session: Instantiates a session inside a cloud connecting it to real systems.

OCEAN framework software architecture takes advantage of Hypervisor and ContainerBased virtualization technology (see Figure 4.4) allowing the orchestration between applications using a Cloud Application Program Interface (API) and Docker API together.

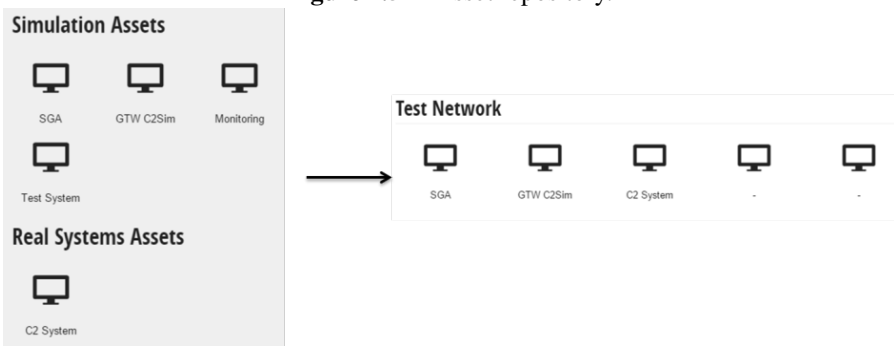
4.6.1 Assets Repository

User select assets from a marketplace-like repository of simulation and real systems, as shown in Figure 4.5. For example, users could create a simulation environment and translate simulation data from/to Command & Control/ Command data with a Command and Control Simulation Stimulation Gateway (translator) service.

4.6.2 Scenario Service

A Representational State Transfer (REST)-based technology service prototype manages a synthetic environment CGF application (Scenario) through a web inter-

Figure 4.5 Asset repository.



face. All applications and services could be managed by similar interfaces, as shown in Figure 4.6.

4.6.3 Web Viewer

A web viewer is used to monitor and control the simulation environment from any location and with any device like a smartphone or a tablet. The interface resides in a web browser and it is operating system agnostic. (Figure 4.7)

4.6.4 Security

At the beginning, the OCEAN project will be deployed on a cloud infrastructure based on Openstack VMware Solution. From the security perspective, it should be specifically noted that OpenStack has not undergone a Common Criteria certification, however VMware have achieved Common Criteria Certification. As a possible security baseline solution the system will be installed by separating the client network from the one used by the virtual systems involved preventing the possibility to access the real data.

4.7 Use Cases

According to the experiments and the experience in which the M&S CoE is involved, it could be possible to reuse other projects run by the M&S CoE to provide already developed and well-proved use cases for MSaaS experimentation activities. In particular, an identified use cases for study is the Urbanization Project ”Archaria” model.

Figure 4.6 Web interface for scenario generation service.

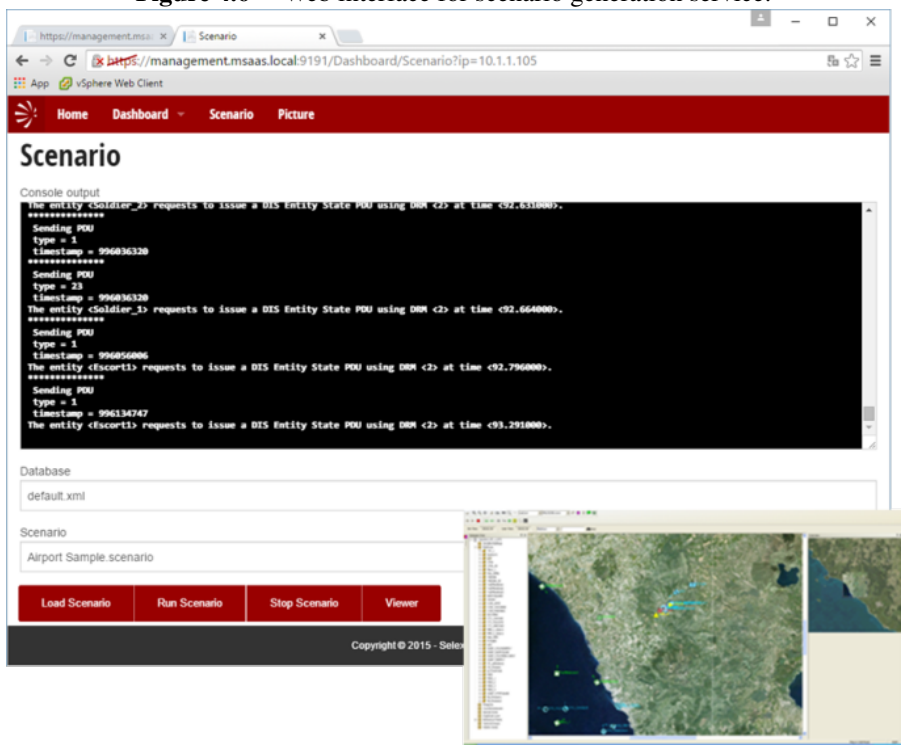


Figure 4.7 Web viewer.

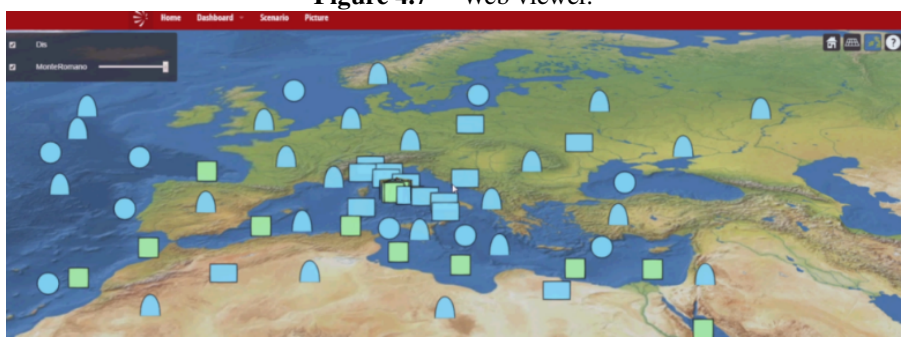
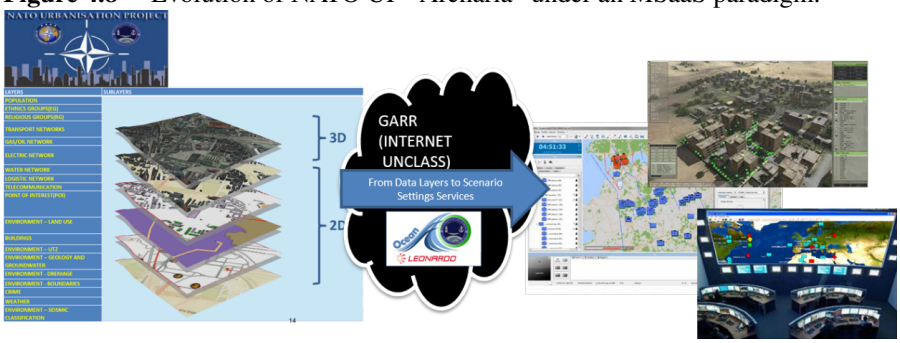


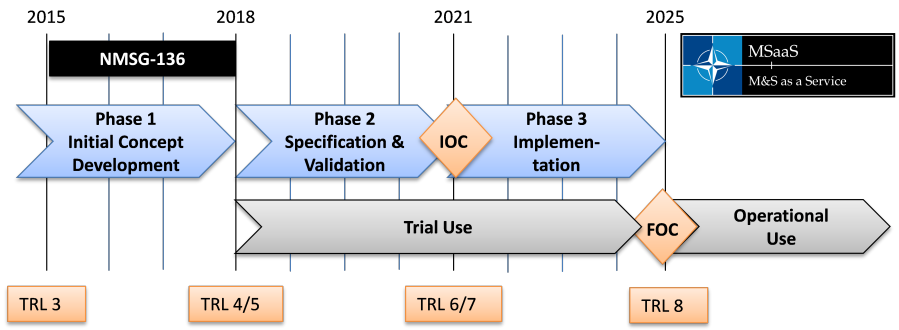
Figure 4.8 Evolution of NATO UP "Archaria" under an MSaaS paradigm.



4.7.1 Urbanization Project (UP)

The NATO ACT Urbanization Project (UP) [23] is an example of ACT CD&E activity to conduct an Urbanization Conceptual Study and Experiment to examine the impact on NATO military operations of potential crises in urban areas and consequences of Urbanization in 2035. The M&S CoE was tasked in this framework to develop a model for a future city, representing an urban environment, which could be the terrain for different kinds of instability scenarios, like megacity turmoil, large scale disaster and disruptive impacts of migration, as defined within the Framework for Future Allied Operation (FFAO). Several layers of the megacity were designed and filled with relevant data, considering different aspects of the urban environment like roads, transportations, communications, utilities, etc. All of these layers, about 250 modelled and filled with data, can be reused to generate scenarios settings services to provide a set of large urbanized area simulation, as shown in Figure 4.8.

Figure 4.9 MSaaS Implementation plan.



4.8 Conclusions

The M&S CoE with Leonardo and other upcoming industrial and academic partners, which are joining the project under the OPEN SIMLAB initiative, have started to design and develop an initial MSaaS Prototype called OCEAN. According to the administrative and technical timing needs of the NMSG 136 MSaaS Implementation Roadmap, shown in Figure 4.9, the initial deployment at the M&S CoE of the OCEAN solution prototype providing embryonic MsSaaS services will be implemented no later than the end of 2016 with goals of leveraging existing experiments, such as UP "Archaria", to demonstrate the value of MSaaS. Regarding the concept development and experimentation phase and related Verification and Validation (V&V) activities, a viable way to proceed could be to identify the right experimentation and exercise events to perform V&V activities at least once a year. The CWIX event could be one of the best experimentation venues where it is possible to experiment and verify MSaaS services before their validation and implementation. Regarding the validation and accreditation of MSaaS services, a large exercise event like Trident Juncture, Steadfast Cobalt or Viking could be the right venue for MSaaS services validation and accreditation before their implementation (IOC).

Acknowledgments

Special thanks go to the M&S CoEs partners and to the NMSG 136 members. They made it possible to start to developing this exciting and challenging project.

REFERENCES

1. NATO Allied Council, "NATO Modelling and Simulation Master Plan", NATO document, (2012).

2. NATO Science and Technology Organization, "The NATO Modelling and Simulation Group", [Online]. *Available: https://www.sto.nato.int/Pages/modelling-and-simulation.aspx* [Accessed June 2016], (2016).

3. NATO Science and Technology Organization, "MSG 136: Modelling and Simulation as a Service. STO CSO - STO activities", [Online]. *Available: http://www.cso.nato.int/activities.aspx?RestrictPanel=5* [Accessed May 2016], (2016).

4. North Atlantic Military Committee, "MC 0583 - MC Policy for NATO Concept Development and Experimentation", Brussels, Belgium: NATO document, (2009).

5. NATO Science and Technology Organization, MSG-136, "Operational Concept Document (OCD) for the Allied Framework for M&S as a Service DRAFT", NATO document, (2016, June 10).
6. Ministry of Defence, Chief Technology Officer, "Defence information and communications technology strategy", UK: Document, (2013).
7. Department of Defense, Chief Information Officer, "Cloud Computing Strategy", Washington, D.C. VA, USA: Document, (2012).
8. Stato Maggiore della Difesa, VI Reparto Sistemi C4I e Trasformazione, "SMD–NEC–001 Linee di indirizzo di Modelling & Simulation per lo sviluppo dei Sistemi C4ISTAR della Difesa", Rome, Italy, IDGS document, (2007).
9. NATO NCIA, "NATO's First Step to the Cloud: Overview and Business Drivers", NATO document, (2014).
10. D. Mercier, "The new architect of transformation", *The Three Swords Magazine*, 29/2015, pp. 6-8, Joint Warfare Centre, Stavanger (NOR), (2015).
11. NATO Consultation, Command and Control Board, 'NATO Architecture Framework version 3", NATO document, (2007).
12. The Open Group, "TOGAF, an Open Group standard", [Online]. *Available: http://www.opengroup.org/subjectareas/enterprise/togaf* [Accessed June 2016], (2016).
13. ISO, "ISO/IEC/IEEE 15288:2015, Systems and software engineering - System life cycle processes. ISO/IEC JTC 1/SC 7", International Standard Organization, (2015).
14. R. Siegfried, T. Van den Berg, A. Cramp and W. Huiskamp, "M&S as a Service: Expectations and challenges", *In Fall Simulation Interoperability Workshop*, pp. 248-257, Orlando, FL (USA), (2014).
15. ITIL, "ITIL Glossary", [Online]. *Available: https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_GB-v1-0.pdf*[Accessed June 2016], (2011).
16. ISO, "ISO/IEC 20000-1:2011", [Online]. *Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51986* [Accessed June 2016], (2011).
17. IBM, "What is cloud computing?", [Online]. *Available: https://www.ibm.com/cloud-computing/what-is-cloud-computing* [Accessed June 2016], (2016).
18. VMWARE, "A Performance Comparison of Hypervisors - A performance study", [Online]. *Available: http://www.vmware.com/pdf/hypervisor_performance.pdf* [Accessed June 2016], (2015).
19. P. Zerger, B. Posey and C. Henley, "The Hands-on Guide: Understanding Hyper-V in Windows Server 2012", Veeam, (2012).
20. M. Daconta, "Containers Add New Efficiency To Cloud Computing.", *Information Week. [Online]. Available:*

http://www.informationweek.com/cloud/containers-add-new-efficiency-to-cloud-computing/d/d-id/1112037 [Accessed June 2016], (2013).

21. E. Cayirci, "Modeling And Simulation As A Cloud Service: A Survey", *Proceedings of the 2013 Winter Simulation Conference*, (2013).
22. NATO ACT, C4ISR Technology & Human Factors (THF) Branch, "C3 Taxonomy baseline 1.0", NATO document, (2012, June 15).
23. NATO ACT, "NATO Urbanization Project", [Online]. *Available: http://www.act.nato.int/urbanisation* [Accessed May 2016], (2016).
24. NATO ACT CEI, "NATO Concept Development and Experimentation Handbook", Norfolk, VA, USA: NATO document, (2013).
25. NATO ACT, "2015 Gap Analysis Report on Modelling and Simulation in support of military training", Norfolk, VA, USA: NATO document, (2015).
26. NATO Standardization Agency, "Allied Joint Doctrine - AJP 1.0 (D)", Brussels, Belgium: NATO document, (2010).

CHAPTER 5

COALITION WARRIOR INTEROPERABILITY EXPLORATION, EXPERIMENTATION, EXAMINATION, EXERCISE (CWIX)

Roberto Censori, Alfio Scaccianoce, Fabio Corona

M&S Centre of Excellence

5.1 Overview of the 2017 CWIX M&S Focus Area

The NATO Modelling & Simulation (M&S) Centre of Excellence (CoE) successfully led the M&S Focus Area (FA) at the 2017 Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX). This effort involved coordinating the execution of interoperability tests, avoiding conflicts and overlapping of concurrent activities while maximizing the tests execution and performance. The M&S FA attracted multiple simulation systems from 9 Nations/Organizations including Canada, France, Germany, Hungary, United States, the Joint Multinational Simulation Centre (JMSC), the NATO Joint Force Training Center (JFTC), the NATO Joint Warfare Center (JWC) and the NATO M&S CoE. The objectives for the M&S FA were identified as below:

1. Federate different types of networked simulation systems building a complex federation facilitated by NATO MSG-134's Integration, Verification and Certification Tool and associated processes.
2. Provide simulation services both inside and outside the FA according to NATO MSG-136's Modelling and Simulation as a Service paradigms and architecture.
3. Stimulate real C2 Systems by actively supporting the Joint Vignette.

The M&S FA managed a complex federation composed of different subnets based on both the Distributed Interactive Simulation (DIS) and High Level Architecture

(HLA) standards.

During the exercise, the main challenge was to configure each simulation system to provide and consume simulated entities with other participants. This was challenging due to the number of different Federated Object Models (FOMs), communication protocols and message formats and entity type mappings and databases alignments necessary in to adapt with other capabilities. Technical personnel from industry made a significant effort to overcome software limitations that were preventing the interoperability among simulation systems. In this context, a key role was played by a M&S multi-protocol gateway to overcome this unexpected interoperability issue through the development of code on site.

The M&S FA's federation of simulators provided simulated objects to the NATO Common Operating Picture (NCOP) and a real time Full Motion Video from a simulated UAV, which provided a 3D visualization of what was happening in the area of operations (virtual reality). These tests proved the interoperability, flexibility and adaptability of M&S capabilities and their ability to interoperate with the Command & Control (C2) systems using different format/protocols. The M&S systems also demonstrated the capability to interoperate and provide extensive simulation services to a wide range of Partners. Through the success of these interoperability test cases with C2 systems, the M&S FA proved how simulation services can support the Commanders and their Staffs training during the exercises, as well as their decision making during operations, or the prediction, experimentation and development of new concepts of operations, doctrine and procedures. Despite the fact that the CWIX 2017 objectives were quite ambitious, the M&S FA proved the capability to fully accomplish them. This indicated that there is room enough for more challenging objectives during the next CWIX.

5.2 Initiative over CFBLNet — Brief report

5.2.1 Capability description

The remote initiative over CFBLNet was played with the Live Virtual Constructive C2 Gateway (NATO-MSCOE-LVC GTW Remote) system, which is a multi-protocol translator for distributed simulations and a bridge for NATO C2 systems. It can join different M&S federations, translate entities and interactions using different protocols and re-distribute information. NATO-MSCOE-LVC GTW enables the connection among different M&S federations that use different object models (FOM), technologies (RTI) and protocols (DIS, HLA, HLA evolved). It controls and adapts data exchange in real time. It is a central node to integrate large-scale simulations, connecting heterogeneous live, virtual and constructive environments at the same time. The system is produced by VITROCISET company.

NATO-MSCOE-LVC GTW Remote can also feed NATO C2 systems with simulation data from a remote location using the following standard protocols:

- NFFI 1.3.1 (both IP1 and IP2)
- MIP DEM Block 3.1

5.2.2 Interoperability Achievements

The NATO-MSCOE-LVC GTW REMOTE (located in Rome) tested 2 main components: LVC Gateway and C2Bridge (NFFI and MIP DEM Block 3.1). As an LVC Gateway, NATO-MSCOE-LVC GTW REMOTE tested the following function:

- get data from a simulation program (DIS v.6) and transmit to a CONSUMER located in JFTC.
- get data from a simulation program (DIS v.6) and feed the local component C2Bridge.

With the component C2 Bridge, NATO-MSCOE-LVC GTW performed the following operations:

- created NFFI (IP1 and IP2) server and established a connection with POL-BMS JASMINE@CWIX 2017.
- Data from simulation environment, collected by Gateway component, was transmitted to CONSUMER.

Data received at the remote from a DIS simulator was sent to NATO-MSCOE-LVC GTW and to the LAND C2 system TUR-DOOB4.0-BILATERAL with protocol MIP DEM block 3.1. The remote also exchanged symbols and other graphic objects. In this way, NATO-MSCOE-LVC GTW REMOTE reproduced by itself the typical activities of a whole reporting organization.

5.2.3 Interoperability Challenges

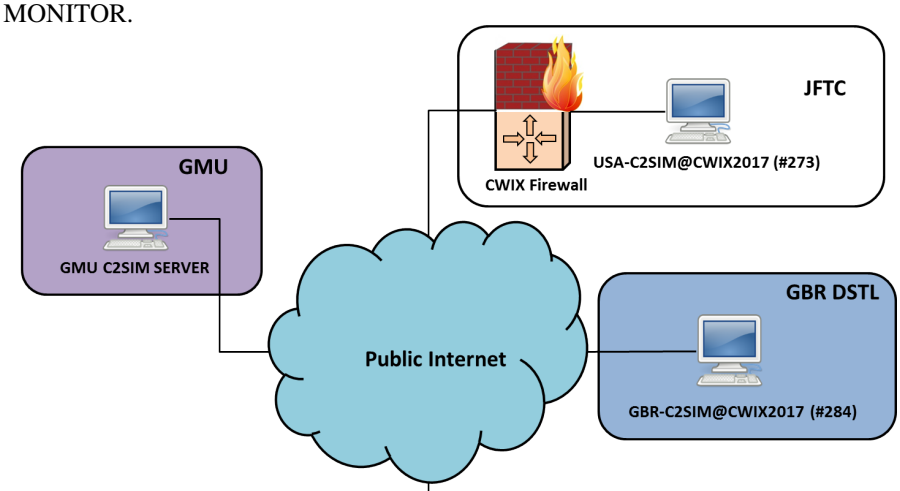
NATO-MSCOE-LVC GTW REMOTE also tried to federate the capability NATO-MSCOE-LVC GTW (from JFTC) into a common HLA federation (MÄK RTI 4.0.4). While federation was accomplished, the data was incomplete. This issue will be explored further next year.

5.3 Initiative with MSG-145 partners on C2Sim over Unclassified Network — Brief report

5.3.1 Capability description

An initiative with MSG-145 partners on C2-Sim Interoperability Language over an Unclassified Network was played with the C2SIM REMOTE MONITOR, which is a capability to verify the operation and results during exchange of Order, Request and Report information among coalition C2 and simulation systems, with a possible insertion of cyber effects. The message exchange was implemented in the standards-based interoperability language C2Sim. The monitoring was performed on the George Mason University (GMU) C2Sim Server during the tests between USA Army Modelling and Simulation Office (AMSO) C2Sim and UK Defence Science and Technology Laboratory (DSTL) capabilities, as in the architecture illustrated in Figure 5.1 .

Figure 5.1 Network architecture of the CWIX tests involving C2SIM REMOTE MONITOR.



Port #	Data
80	HTTP
61613	STOMP
8080	REST

5.3.2 Interoperability Achievements

The NATO-C2Sim Remote Monitor (STOMP listener) participated as an observer capability, remotely connected on the unclassified network, checking the correct operation of the C2Sim Server located at the George Mason University in Fairfax, VA (USA). During the tests, the USA-C2SIM@CWIX2017 capability (a surrogate C2 software, called BMLC2GUI by the GMU) pushed C2Sim orders to UK-located GBR-C2SIM@CWIX2017 (JSAF), which processed them correctly and produced C2Sim reports. The reports were correctly processed by the C2Sim Server and, then, received and displayed on USA-C2SIM@CWIX2017. The same success was repeated when cyber effects were added to delete part of the reports. Throughout the testing, C2Sim Remote Monitor interoperated successfully.

5.3.3 Interoperability Challenges

The NATO-C2Sim Remote Monitor (STOMP listener) operated as expected, but it was able to visualize only the reports processed by the C2Sim server. Future improvements for increasing the interoperability and functionality of this capability should include the possibility to control also the exchange of C2Sim orders through the C2Sim Server.

5.3.4 Improvements from previous CWIX

This is the first participation of capabilities focused on experimentation on C2Sim Interoperability Language, so, even if the testing was a little bit limited, it was an enormous step forward towards the operationalization of this standard being developed by the Simulation Interoperability Standards Organization (SISO), in collaboration with the MSG-145 research task group of the NATO Modelling and Simulation Group (NMSG).

CHAPTER 6

IMPLEMENTATION OF THE NATO LESSONS LEARNED PROCESS IN THE MODELLING AND SIMULATION DOMAIN

WALTER DAVID, JASON JONES[1] AND THOMAS LASCH[2]

[1]M&S Centre of Excellence, Rome, Italy
[2]US Army/ Joint Multinational Simulation Center (JMSC) Grafenwoehr, Germany

This paper was presented in occasion of the 2017 International Forum for the Military Simulation, Training and Education Community (ITEC), Rotterdam Ahoy, 16-18 May 2017

6.1 Introduction

According to AJP-3(B) Allied Joint Doctrine for the Conduct of Operations, ''*the purpose of the Lessons Learned (LL) capability in NATO is to learn efficiently from experience and to provide validated justifications for change(s) in order to improve performance*" [1]. Important elements enable the LL capability and include strong leadership support, a positive mindset, internal and external LL processes and a structure including trained and skilled people, tools and knowledge sharing. The aim of the LL capability is to reduce operational risks and improve cost efficiency and operational effectiveness. As the key part of the NATO LL capability, the NATO LL process has been established through policy and doctrine and is also largely adopted by national militaries for providing improved capability in the domains of doctrine, organisation, training and education, operation, concept development, experimentation.

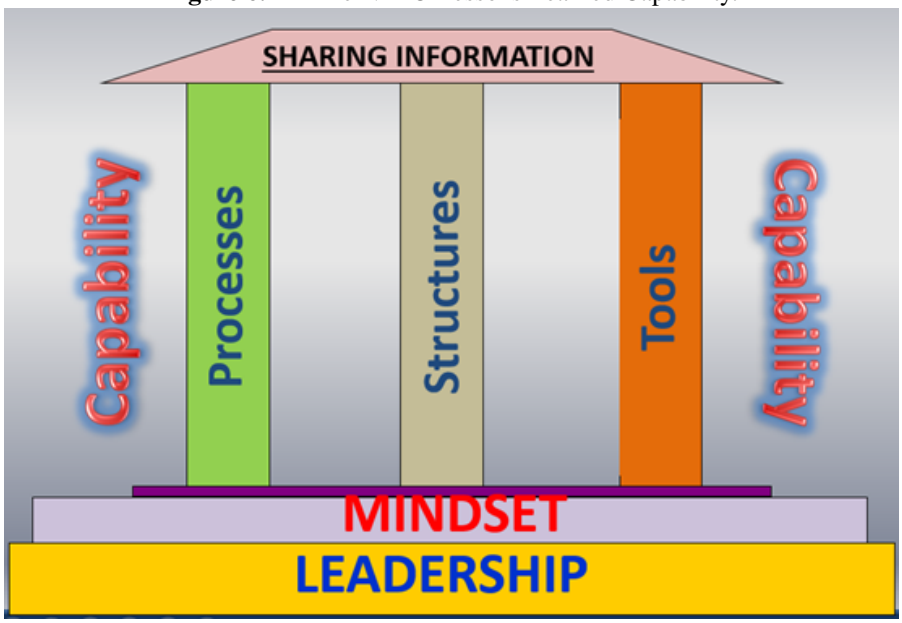
Although LL processes are commonly used in this capability development aspect, we have observed a lack of a similarly standardized way in which we develop, use and improve technical and, more specifically, Modelling and Simulation (M&S) ca-

pabilities. This is due, in part, to the informal and ad-hoc way in which M&S related observations and lessons are gathered and disseminated. More specifically, several M&S-focused entities gather lessons through both formal and informal processes.
M&S forums, workshops, groups and sub-groups share best practices and other post-event feedback mainly only among their members. M&S related information is commonly made available to experts, developers and users through e-mail and/or scattered repositories.
But a more formal mechanism and a standardized process could significantly improve the sharing of information, expand the reach to the M&S community and provide a better return on investment for NATO and nations. In support of the LL capability, the NATO–accredited Centres of Excellence (COEs), as nationally/multinationally sponsored entities, offer recognized expertise and experience to the benefit of the Alliance. One of the pillars of excellence that the Centres are supposed to provide in support to Alliance transformation is the Analysis & LL. In particular, the M&S COE's mission is to support NATO and its Nations by providing subject matter expertise on all aspects of modelling and simulation activities. The Analysis & LL Section of the M&S COE has been tasked to create and maintain a repository of collected M&S best practices and lessons learned, to identify M&S requirements to support concept development and experimentation and assist Allied Command Transformation and NATO Science & Technology Organisation/NATO M&S Group (NMSG) in the identification of NATO and national M&S Capability Gaps.

6.2 The NATO Lessons Learned capability and the Lessons Learned process

Organisations that are continuously transforming themselves and that facilitate the learning of theirs members are considered *learning organisations* [2]. The process of learning, according to Nick Milton in his "The Lessons Learned Handbook" [3] is characterized by three phases: the Identification (collecting learning from experiences); the Action (taking action to change the existing ways of doing things based on the learning); and the Institutionalization (communication about the change for the benefit of the organization). In NATO, the institutionalization of learning would be translated to lessons sharing and incorporation into doctrine and procedures.
Therefore, through a formal approach to learning, individuals and the organization can reduce the risk of repeating mistakes and increase the chance to repeat successes. In the military context, this means reduced operational risk, increased cost efficiency and improved operational effectiveness [4]. The Bi-SC Directive 080-006 Lessons Learned [5]defines a LL capability as a "*capability that provides a commander with the structure, process and tools necessary to capture, analyse and take remedial action on any issue and to communicate and share results to achieve improvement.*"
The key elements (see Figure 6.1 1 from the Bi-SC Directive) of a LL capability are represented as structure, process and tools pillars, to support information sharing.

Figure 6.1 The NATO Lessons Learned Capability.



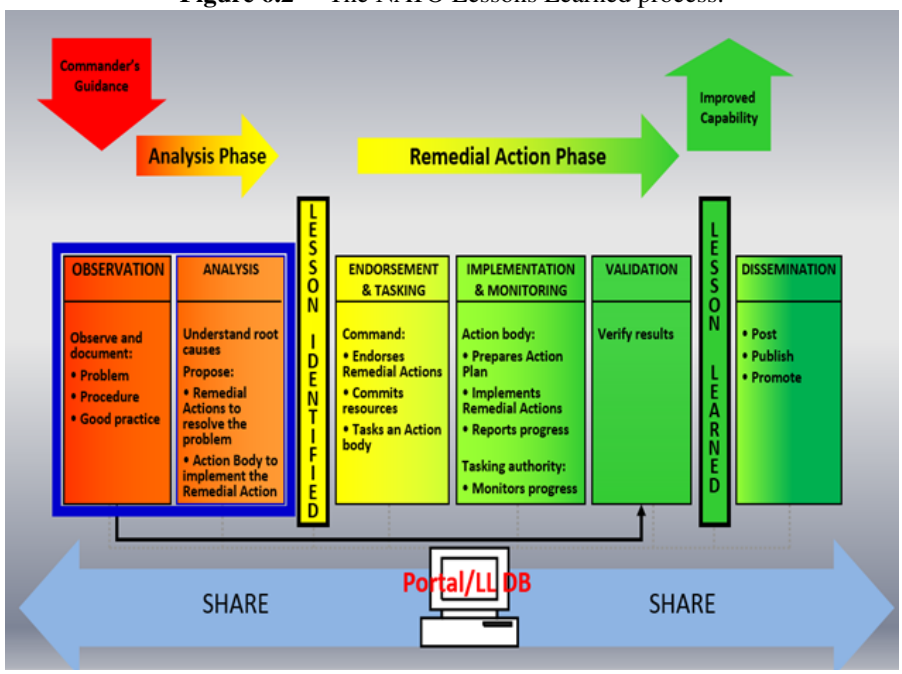
The Mindset and Leadership are the fundamental cultural and social elements that are required in the organization for implementing an effective LL capability but it is only with the Information sharing that we can ensure the effective functioning of the capability.

The LL processes are the internal and external procedures for the writing, analysis and staffing of the observations collected during an exercise, operation, experiment or generally an activity until a lesson learned is produced. Figure 6.2 illustrates the LL process used by NATO in order to support the LL capability, as given in the Bi-SC Directive 080-006. If we overlay Nick Miltons three phases of learning with the NATO LL process, we see that ”Identification” occurs during the Analysis phase of the process; ”Action” and ”Institutionalization” occur during the Remedial Action phase. In NATO, ”Institutionalization” is considered as an integral part of the action requested to produce a Lesson Learned.

6.3 Best Practices and Lessons Learned in M&S

As LL practitioners, we face many obstacles including lack of sharing, lack of high level support, poor mindset, habit to working in silos, poor internal communication, and rigid bureaucracy. In the specific M&S domain there are even more challenges as no policy is in place in order to standardize the way in which we

Figure 6.2 The NATO Lessons Learned process.



develop, use and improve M&S capabilities. M&S-focused entities gather lessons through formal/informal processes. Forums, workshops, groups, sub-groups share best practices and post-event feedback generally in a non-standardised format and only with their members.
Relevant information is often made available only through e-mail. Lessons identified/learned may be stored in scattered repositories, classified databases, thus making the access virtually impossible for the wider community of military users.
The M&S COE used active data collection methods in its analysis research, in particular surveys and interviews with stakeholders/shareholders mainly conducted during meetings and events (CAX Forum, NMSG business meeting, etc.). Identified obstacles to LL in M&S include disconnection or lack of mutual interest between the LL and M&S experts' communities. During a recent MSG-146 *Simulation for Training and Operation Group Land (STOG-L)* meeting, April 2017, the feedback from a survey delivered during the LL workshop highlighted that LL processes in Nations exist but in the specific M&S domain best practices and lessons learned are generally not available or known by M&S military users (in the 80% of returned questionnaires).
From direct observations and interviews, we noticed that M&S experts in simulation centres are often not using the NATO approved ODCR (Observation-Discussion-Conclusion-Recommendation) standard format for collecting observations. They are focused on fixing the problems, then eventually writing log reps which are generally kept internally in the CAX support teams in the case of Computer Assisted Exercises (CAX).
On the other side, LL officers are mainly focused on operations, training and education not considering the problems in simulation as a priority. Often classified networks are used for unclassified lessons; the observations are mainly written in national languages thus not easily ready for sharing in the Alliance and with partners. But the interest for an efficient sharing mechanism can be high: in a survey conducted during NATO CAX Forum in Ottobrunn-Munich (Germany), September 2016, 46% of respondents provided positive feedback on their availability to be involved in a future M&S LL Capability Team and to take part to an eventual specialised M&S LL seminar/conference.

6.4 Why a LL Capability in M&S domain?

If the M&S community in NATO is expected to identify, understand and analyse M&S related capabilities and gaps on a continuing basis, then a more formal standardized process should be established to collect and analyse M&S LL, requirements and future developments. Our ability, as the M&S community, to support and to meet operational requirements and mitigate risks will continue to transform as new capabilities are developed and new threats to security and stability are emerging and challenging our decision making processes, from the hybrid and cyber warfare to the environmental and climate change impact. We must constantly seek to im-

prove through a continuous process of identifying lessons, conducting analysis, implementing solutions and capturing these elements for more effective sharing across the community.
The potential benefits from managing lessons learned for the modelling and simulation community are significant. The highly technical nature of modelling and simulation, the frequent changes to software and networks, combined with the similarity of tasks across the various NATO and Nation simulation centres increases the likelihood that multiple centres experience similar problems. The ability to share these lessons and best practices allows the focus to be on conduct of the event rather than troubleshooting set-up and interoperability issues. As further evidence that a formal LL process for M&S related lessons can benefit the Alliance, we note that the LL process has been successfully implemented, for the first time, in the *Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise* CWIX 2016 M&S Focus Area led by M&S COE and has provided valuable feedback for the improvement of CWIX 2017 starting the remedial action addressing the identified problems from the Initial Planning Conference.

6.5 Building a LL Community of Interest for M&S

The NATO LL process is an excellent starting point to establish a formal NATO-wide M&S-focused LL process. If implemented effectively, the process would overcome scattered information and other obstacles to sharing best practices and lessons learned. A LL capability implemented in the M&S domain could serve as the primary means of capturing requirements, identifying and mitigating gaps and providing a centralized repository for all M&S related lessons learned, capabilities and requirements. This will further enable groups in the NATO Science and Technology Organisation (STO) such as the MORS, STOG and the wider M&S community to share information in a more dynamic fashion, rather than through infrequent, but burdensome efforts.
As a NATO Centre of Excellence with a wide array of modelling and simulation subject matter expertise, the M&S COE is well positioned to recommend and implement a solution for collecting and managing lessons learned across the NATO and national enterprise. As a COE, not belonging to the NATO Common Structure (NCS), the Centre is unconstrained by NATO or national structures, allowing it to be selective in choosing where to maintain this material.
The M&S COE selected the NATO JALLC as the host for M&S community of interest based on its capabilities and accessibility to a large number of users while maintaining protections for the communitys data. From 2016 the M&S COE is the administrator of the Modelling and Simulation Lessons Learned Community of Interest (M&S COI) on the unclassified NATO LL Portal (NLLP) managed by JALLC and promoted it at the annual NATO Computer Assisted Exercise (CAX) Forum, NATO M&S Group meetings and an array of other digital media. The intended use

of the M&S COI portal is to become the major venue for sharing observations, best practices and lessons among users from centres of excellence, simulation centres and other accredited agencies and organizations on the use of M&S applications to support training, education, exercises, operations, concept development and experimentation. The M&S COI has been initially fed by lessons collected from the CWIX 2016, other relevant documents, papers, articles and presentations for NATO Science & Technology Organisation/ MORS/NATO M&S Group (NMSG).

6.6 Conclusions and way ahead

M&S Community of Interest (M&S COI) looks to strengthen the connection between the M&S COE and M&S users from NATO and Nations and expanding this reach to the wider military M&S users' community [12]. However, users will not come to the M&S COI portal if there is not enough valuable content to generate interest, therefore the availability of contributions from NATO and Nations is essential for that to happen. NATO and Nation M&S users must participate in the M&S COI in the NATO LL Portal (NLLP) managed by JALLC.

The M&S COE challenge was, and continues to be, changing the habits of NATO and some national simulation centres who are maintaining their best practices and lessons learned in organizational/national/classified repositories. As a lessons learned professional, it was encouraging to see these organizations capturing their lessons and best practices; unfortunately, these organisations' individual internal processes restricted them from sharing with the larger community.

Unlike the JALLC portal, the national networks and domains holding these lessons limit access to personnel from that organization and/or nation. While exceptions may be allowed, they require significant effort from all parties to enact. As for the lessons stored on classified networks, access is restricted to a defined group of people. Most frustratingly, many of the lessons associated with managing and controlling modelling and simulations are actually unclassified. Those organizations were placing these predominantly unclassified lessons on classified networks simply because that was the network for the simulation event.

These factors have made it difficult so far for the JALLC-based M&S Community of Interest to expand its user base. Therefore, in the coming months, the M&S COE is going to propose the creation of a M&S Lessons Learned Capability Team that will bring together NATO and national simulation centres to explore and implement solution(s) that better support the intent of NATO lessons learned — capturing, sharing and improving NATO and Nations' capabilities.

Acknowledgments

We have to express our appreciation to Ms. (NATO Civ.) Katie Mauldin, Senior Operational Research Analyst, Joint Analysis and Lessons Learned (JALLC) Lisbon, for sharing her pearls of wisdom thus improving the manuscript significantly.

REFERENCES

1. NATO Standardization Agency, "Allied Joint Doctrine for the Conduct of Operations - AJP 3(B)", Brussels, Belgium: NATO document, (2011, March).
2. M. Pedler, J. Burgogyne and T. Boydell, "The Learning Company: A strategy for sustainable development", *2nd Ed., McGraw-Hill*, London, (1997).
3. N. Milton, "The Lessons Learned Handbook: Practical approaches to learning from experience", *1st Ed., Chandos Publishing*, ISBN 978843345879, (2010).
4. NATO Joint Analysis and Lessons Learned Centre (JALLC), "The NATO Lessons Learned Handbook 3rd Edition", Lisbon, Portugal: NATO document, (2016, February).
5. NATO, "Bi-SC Command Directive (Bi-SCD) 080-006 Lessons Learned", NATO Unclassified document, (2013, July 10).
6. NATO ACO, "ACO Directive 080-001 Lessons Learned", NATO Unclassified document Releasable to PfP/ISAF/KFOR, (2013, April 8).
7. NATO, "Bi-SC Collective Training and Exercise Directive (CT&ED) 075003", NATO Unclassified document, (2013, October 2).
8. North Atlantic Council, "NATO Primary Directive on Information Management C-M(2008)0113(INV)", NATO Unclassified document, (2008, November 27).
9. NATO Joint Analysis and Lessons Learned Centre (JALLC), "Joint Analysis Handbook 4th Edition", Lisbon, Portugal: NATO document, (2016).
10. M. Saunders, P. Lewis and A. Thornhill, "Research Methods for Business Students", *4th Ed., Prentice Hall*, ISBN 9780273701484, (2007).
11. NATO, "Bi-SC Alternative Analysis Handbook (AltA)", NATO Unclassified document, (2012, December 7).
12. W. David, "Challenges and Opportunities: establishing a Lessons Learned Community for Modelling and Simulation", *Proceedings of NATO Lessons Learned Conference*, Lisbon, Portugal, (2016).
13. NATO, "The NATO Lessons Learned Policy MCM-0021-2011", NATO Unclassified document, (2011, May 18).

APPENDIX A
M&S TOOLS

Table A.1 ArcGIS for Server

Name	ArcGIS for Server
Version	10.5.1
Manufacturer	ESRI
Type	Other
Application Area	Terrain generation and analysis
Description	ArcGIS for Server connects people with the geographic information they need to make better business decisions. Esri GIS Web server software improves workflows and resource tracking using Web mapping applications and services that you can distribute throughout your organization.
Federability	No
Extensions	Network analyst; 3D analyst; Image; Schematics; Geo event; Spatial analyst.

Table A.2 ArcGIS for Desktop Advanced

Name	ArcGIS for Desktop Advanced
Version	10.5.1
Manufacturer	ESRI
Type	Other
Application Area	Terrain generation and analysis
Description	Professional GIS software for creating maps, conducting spatial analysis and sharing intelligent visualizations for better decision making.
Federability	No
Extensions	3D analyst; ArcStorm; ArcStormEnable; MrSID; Network analyst; Plotting; Publisher; Spatial analyst.

Table A.3 Extend Sim Suite

Name	Extend Sim Suite
Version	8
Manufacturer	Imagine That Inc.
Type	Other
Application Area	Enterprise and System Architecture Simulation
Description	Extend Sim is a powerful, leading edge simulation tool. Using Extend Sim, you can develop dynamic models of existing or proposed processes in a wide variety of fields. Use Extend Sim to create models from building blocks, explore the processes involved, and see how they relate. Then change assumptions to arrive at an optimum solution. Extend Sim and your imagination are all you need to create professional models that meet your business, industrial, and academic needs.
Federability	No

Table A.4 The Joint Conflict and Tactical Simulation

Name	JCATS
Version	12
Manufacturer	Lawrence Livermore National Laboratories
Type	Constructive
Entities	Dynamically aggregated and de-aggregated, mounted and dismounted systems at various hierarchy levels
Application Area	Training & Exercise; CD&E
Description	The Joint Conflict and Tactical Simulation (JCATS) is a discrete event, constructive simulation that simulates actions and events of people and systems in specified environments. Its interactive design enables operators to initiate and influence events, although outcomes are stochastically determined utilizing user-defined statistical data. JCATS simulates the 'effects' of actions and events to simulate combat at the entity level. JCATS is data-driven, which enables users to rapidly define and refine their scenario parameters to ensure realistic simulation of their specific scenario.
Federability	Yes
Interoperability standards with Simulators	HLA 1.3; HLA 1516; HLA 1516 2010
Interoperability standards with C2	link16; OTHGOLD; ADATP-3

Table A.5 The Joint Theater Level Simulation

Name	JTLS
Version	4.9
Manufacturer	Roland Associated
Type	Constructive
Entities	Units and targets as basic entities; the user-configurable database defines unit sizes, combat systems, supply categories, and militarily significant targets to be represented; the scenario database can be developed to represent the requisite detail for systems of interest within this unit structure
Application Area	Training & Exercise; CD&E
Description	The Joint Theater Level Simulation (JTLS) is an interactive, Internet-enabled simulation that models multi-sided air, ground, and naval civil-military operations with logistical, Special Operation Force (SOF), and intelligence support.
Federability	Yes
Interoperability standards with Simulators	HLA 1.3; HLA 1516; HLA 1516 2010
Interoperability standards with C2	link16; OTHGOLD; ADATP-3

Table A.6 Multi Data Link Processor (MDLP)

Name	Multi Data Link Processor (MDLP)
Version	06d
Manufacturer	Leonardo company
Type	Other
Application Area	C2 systems–simulators interface
Description	The Multi Data Link Processor (M-DLP) is an interoperable and scalable Multi-Link Integration Solution. M-DLP supports data link protocols and standards such as: ▪ Link11 A/B; ▪ Link16; ▪ Link22; ▪ JREAP; ▪ VMF; ▪ DIS.
Federability	Yes
Interoperability standards	HLA; DIS; link16; OTH Gold; ADATP-3; NFFI.

Table A.7 Riverbed Steel Central (formerly OPNET)

Name	Riverbed Steel Central (formerly OPNET Modeler)
Version	16
Manufacturer	Riverbed
Type	Other
Application Area	Communications and Networks simulation
Description	Professional communication and network simulator, suitable also for simulation of cyber effects on later versions (i.e., n. 18)
Federability	Yes
Interoperability standards	HLA
Extensions	Wireless; Terrain Modeling; HLA Interface Module, Single Sim.; Sistem-In-The-Loop (SITL)

Table A.8 Scenario Generator Animator (SGA)

Name	Scenario Generator Animator (SGA)
Version	2013
Manufacturer	Leonardo company
Type	Constructive
Number of entities	Up to hundreds of entities out-of-the-box, with built-in doctrines and AI
Application Area	Training & Exercise; CD&E
Description	Scenario Generator and Animator (SGA) is a software tool that lets you build a tactical database and then simulate dynamic, interactive, complex, and real-time tactical and operational environments. These environments, called scenarios, contain individual platforms (such as planes, ships, trucks, radar sites) that interact through detection, communication, engagement and/or destruction. Platforms may be equipped with weapons, such as guns, artillery, and missiles, and other defining characteristics. SGA is based on COTS STAGE (Presagis, Inc.) and includes a lot of customization such as: ▪ Special trajectories (i.e. Ballistic Missile trajectory) ▪ Customized sensors (i.e. IFF) ▪ HLA interaction ▪ Customized entities
Federability	Yes
Interoperability standards	HLA 1.3; HLA 1516; HLA 1516 2010; DIS
Terrain formats	OpenFlight; Common DataBase (CDB)

Table A.9 System Architect

Name	System Architect
Version	11.4
Manufacturer	IBM
Type	Other
Application Area	Enterprise Architecture Modelling
Description	IBM Rational System Architect, the industry's leading application for visualizing, analyzing, and communicating your organization's Enterprise Architecture and business process analysis, increases your competitive edge by improving your real-time decision-Making. IBM Rational System Architect enables an "actionable" Enterprise Architecture, one that enhances organizational agility and flexibility by gradually migrating the organization to an optimized future state in manageable time-phased transitions.
Federability	No
Main supported frameworks	NAF; MODAF; DODAF

Table A.10 Terra Vista Pro Presagis

Name	Terra Vista Pro
Version	2007
Manufacturer	Presagis
Type	Other
Application Area	Terrain generation
Description	Presagis Terra Vista is one of the most used terrain generation software in the world. Provide high-fidelity correlated terrain at multiple levels-of-detail (LOD) across a wide range of image-generators and network simulation standards. Gives integrators and database developers the tools they need to handle everything from the extreme scales required for jet simulation to the high LOD necessary for tactical ground applications. A map model is a method of describing points on the Earth. Cartographic data files are stored using one of the following map models: ▪ Projected: data stored using a map projection that describes the surface of the round Earth in a 2D Cartesian (x,y) coordinate systems. ▪ Geographic: data stored as pairs of latitude/longitude values. Coordinates are relative to an ellipsoid model of the Earth. ▪ Geocentric: data stored in a true three-dimentional (x,y,z) coordinate system. A map model is a combination of an ellipsoid which specifies the size and shape of the earth and a datum which specifies a base point from which the latitude and longitude of all the other points are referenced. Common datums: WGS84 (most common); NAD27 (used in older USGS maps); GRS80 (used in new USGS maps); ED50 (common European datum).
Federability	No
Terrain outputs for	VBS2; JCATS; CTDB; SEDRIS

Table A.11 TRENTA recorder and analysis (R/A)

Name	TRENTA recorder and analysis (R/A)
Version	8
Manufacturer	Leonardo company
Type	Other
Application Area	Simulation analysis and recording.
Description	The TRENTA recorder (TR) (also called NETtool) is a multiprotocol message recorder. The NETtool manage a set of recorders, one for each protocol. The messages are saved both on .pcap (.log for HLA) and .txt format. The recorded messages can be replayed on the network. The TRENTA Analysis (TA) is the software that have in charge the analysis of the recording sessions. The TA is able to show the content of recorded messages, and perform simple analysis, searches and filtering
Federability	Yes
Interoperability standards	HLA; DIS; TDL protocols.

Table A.12 Trial Monitoring

Name	Trial Monitoring
Version	10
Manufacturer	Leonardo company
Type	Other
Application Area	Simulation monitoring.
Description	The Trials Monitoring (TM) is a real-time viewer of entities provided by different protocols on an earth representation. The TM contains a collection of modules that allows to analyze and display different messages: ▪ Simulation data – DIS – HLA ▪ Operative data – Link 11 – Link 16 – ADatP-3 – DDS
Federability	Yes
Interoperability standards	HLA; DIS; TDL protocols.

Table A.13 Vega Prime

Name	Vega Prime
Manufacturer	Presagis
Type	Other
Application Area	C2 systems–simulators interface
Description	The Presagis Vega Prime is an advanced visualization toolkit that displays sophisticated simulated environments. Vega Prime is able to: ▪ Monitor how an operative scenario is evolving during tests; ▪ Federate in simulation session and receive information coming from tools that participate to the simulation, using standard protocols such as DIS and HLA; ▪ Display the scene from different points of view, helping post action evaluation; ▪ Handle Meteorological Conditions.
Federability	Yes
Interoperability standards	HLA; DIS.
Terrain formats	OpenFlight; Metaflight; CDB (Common DataBase).

NATO M&S COE