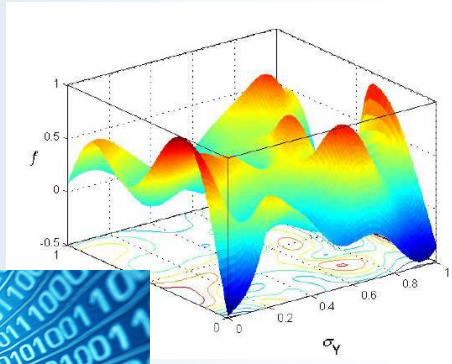
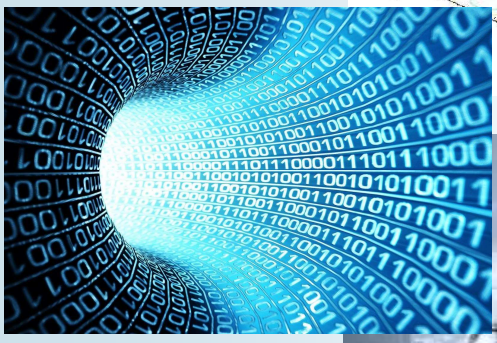
Vol. n. 2 • 2018 ISBN 978-88-942906-4-6

# 2018 Annual Review

NATO M&S COE



NATO Modelling & Simulation Centre of Excellence

# 2018 NATO M&S COE ANNUAL REVIEW

**Edited by**
**NATO Modelling & Simulation Centre of Excellence**


A NATO M&S CENTRE OF EXCELLENCE PUBLICATION

Cover pictures from: ontheradar.foxrothschild.com – “Autonomous Drones – Moral and Ethical concerns”; numeri binari sfondi-pc.com; researchgate.net.



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

Edition: e-book (September 2018)

ISBN 978-88-942906-4-6



Printed in Italy.

Prof. Sebastiano MILARDO, DIEEI, Università di Catania, Italy

Prof. Giacomo MORABITO, DIEEI, Università di Catania, Italy

Ing. Agatino MURSIA, Leonardo company, Italy

Ing. Marco PICOLLO, Leonardo company, Italy

Kai PERVÖLZ, Fraunhofer IAIS (DEU)

Massimo PIZZI, Research and Capability Development Officer in internship (M&S COE)

Prof. Dalibor PROCHAZKA, University of Defence (Brno, CZE)

Lt.Col. Antimo RUSSO, M&S Services Branch (M&S COE)

Maj. Alfio SCACCIANOCE, Experimentation Section Chief (M&S COE)

Lt.Col Stephan SEICHTER, Bundeswehr Office for Defence Planning (DEU)

Viktor STRITOF, CZU/ERS (SVN)

Maj. Cristian TONDO, CIS Section (M&S COE)

Alexander ZIMMERMANN, Fraunhofer IAIS (DEU)

# 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 second Annual Review. This Annual Review provides articles and summaries of selected research, studies and events that took place this year.

This year's review shows our continued work towards establishing an M&S as a service architecture, discusses our several of our efforts within the Cyber and Autonomous System domains, provides details on the courses we have conducted over the last year and provides an overview from our role leading the M&S Focus Area during NATO CWIX.

As a NATO Centre of Excellence our purpose is supporting 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, to show our efforts to make our work more widely available and thus advance the capabilities of NATO, its Nations and partner nations. 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, 2018*

# Acronyms

| | |
|---|---|
| **ACT** | Allied Command for Transformation |
| **AI** | Artificial Intelligence |
| **ATO** | Air Task Order |
| **C2** | Command & Control |
| **CBML** | Coalition Battle Management Language |
| **CBRN** | Chemical Biological Radiological and Nuclear |
| **COE** | Centre of Excellence |
| **COTS** | Commercial Off-The-Shelf |
| **CP** | Command Post |
| **DIS** | Distributed Interactive Simulation |
| **DSEEP** | Distributed Simulation Engineering and Execution Process |
| **DTAG** | Disruptive Technology Assessment Game |
| **GSD** | Guidelines for Scenario Development |
| **GUI** | Graphical User Interface |
| **HLA** | High Level Architecture |
| **LDM** | Logical Data Model |
| **M&S** | Modelling and Simulation |
| **MSDL** | Mission Scenario Definition Language |
| **NAF** | NATO Architectural Framework |
| **NATO** | North Atlantic Treaty Organization |
| **NFFI** | NATO Friendly Force Information |
| **NMSG** | NATO Modelling and Simulation Group |
| **OV** | Operational View |
| **PDG** | Product Development Group |
| **R2CD2** | Research on Robotics Concept and Capability Development |
| **RTI** | Real-Time Infrastructure |
| **SISO** | Simulation Interoperability Standard Organization |
| **STO** | Science and Technology Organization |
| **UAV** | Unmanned Aerial Vehicle |

**UGV** Unmanned Ground Vehicle

# Part I

# PAPERS

# 1. MODELLING AND SIMULATION AS A SERVICE FROM END USER PERSPECTIVE[1]

Lt.Col. Marco Biagini, Lt. Col. Jason Jones, Lt.Col. Michele La Grotta, Maj. Alfio Scaccianoce, Capt. Fabio Corona

NATO Modelling & Simulation Centre of Excellence, Rome, Italy

Dr. Dalibor Prochazka

University of Defence, Brno, Czech Republic

Ing. Agatino Mursia, Ing. Marco Picollo, Ing. Christian Faillace

Leonardo Company, Genova, Italy

***Abstract***

*Modelling and Simulation as a Service (MSaaS) is a new approach being explored by NATO Science and Technology Organization (STO) Modelling & Simulation Group (MSG) Panel for a permanently available, flexible, service-based framework to provide more cost effective availability of Modelling and Simulation (M&S) products, data and processes to a large number of users on-demand. This Research Task Group is working on the development of the implementation of this framework, defining policies, stakeholders' roles, services and reference architecture and reference engineering processes. MSaaS can be defined as "enterprise-based level architecture for discovery, orchestration, deployment, delivery and management of M&S services".*

*The University of Defence of the Czech Republic and the NATO M&S Centre of Excellence are investigating and proposing an approach to contribute to the definition of the MSaaS from an End User perspective.*

*The paper proposes definition of M&S Software as a Service (MSSaaS), M&S Platform as a Service (MSPaaS) and M&S Infrastructure as a Service (MSIaaS) to introduce new roles and new business connections taking also into consideration Service Oriented Architecture (SOA) definitions and*

[1] This paper originally appeared in the 2017 Proceedings of the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC)

*those definitions stated in NATO Modelling and Simulation Master Plan (NMSMP). In particular the authors propose a contribution to the definition of the different stakeholders' roles and their relationships, starting from those of the MSG 136 group (M&S Group 136, Modelling and Simulation as a Service) and introducing new roles regarding the End User.*

*In conclusion, this research and study activity proposes, in addition to the existing definitions, a taxonomy comparing roles across service models (MSSaaS, MSPaaS and MSIaaS). Furthermore, the M&S services' classification is analysed in the framework of the MSG 136 Operational Concept draft, in order to identify the services which are to be properly composed and orchestrated to satisfy the End User requirements.*

## 1.1 Introduction

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" (NATO STO MSG 136, 2016, June 10).

MSaaS is a promising approach for realizing next generation simulation environments to support development of M&S military capabilities (NATO Allied Council, 2012). 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 NATO Modelling and Simulation Master Plan (NMSMP) to maximize the effective utilization of M&S (NATO STO, 2016). According to this vision, it is essential that M&S tools are readily accessible to a large number of users as often as possible. To achieve such 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 M&S CoE, its industrial partners and the Czech Republic University of Defense are participating in the development of the MSG-136 deliverables. In particular we are proposing contributions to the Operational Concept Document (OCD) development and supporting the Evaluation Subgroup by developing a test bed prototype to make available to the MSaaS community of Interest a first, experimental cloud-based infrastructure to execute MSaaS experimentation activities: The Open Cloud Ecosystem ApplicatioN (OCEAN) project (Biagini et al., 2016).

This paper illustrates the authors' contributions to the MSG 136 Operation Concept Document, proposing the Stakeholders roles and related M&S

services' definitions. Additionally the OCEAN project and the application of the stakeholders and M&S service models to the MSaaS implemented solution, the OCEAN prototype, are discussed.

## 1.2 The MSaaS Stakeolders and Services Perspective

The MSaaS Stakeholder roles that can be identified in the Allied MSaaS framework, as proposed and further implemented in the OCD, are shown in Figure 1-1.

### 1.2.1 MSaaS Stakeholders

MSaaS Stakeholder categories are derived from the NMSMP:

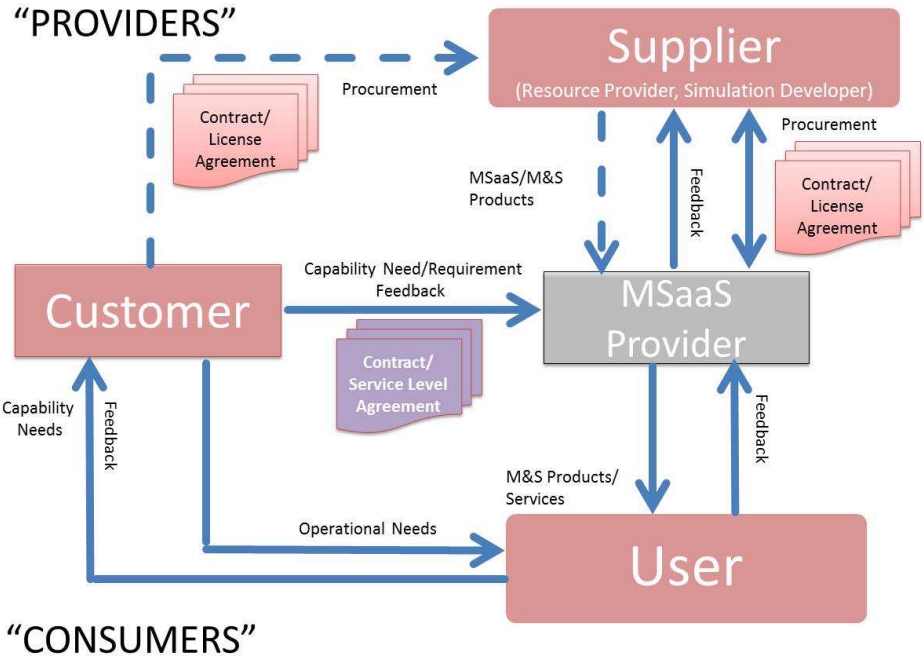



**Figure 1-1: MSaaS Stakeholder Roles in the Allied Framework for MSaaS (NATO STO MSG 136, 2017)**

Customer

The MSaaS Customer is a defense organization with an operational need (e.g. training, mission planning, acquisition), and can include a NATO Nation/HQ/Agency or group of Nations or international entities.

In order to address this need, the Customer may consider the use of MSaaS capabilities available from the Allied MSaaS Framework via a Service

Level agreement (SLA). Alternatively the Customer may procure M&S products and solutions from Suppliers via a contract or license agreement, to be subsequently made available through the Allied MSaaS Framework.

Provider:

In accordance with Customer SLAs, the MSaaS Provider makes M&S products and solutions available to Users from the Allied MSaaS Framework. The MSaaS Provider needs to manage and maintain the Allied MSaaS Framework in order to meet SLAs. This will include the use of 'registry' and 'discovery' services to maintain a repository of M&S products and solutions, either already owned by defence organizations or available from Suppliers through a license agreement, purchase order, another kind of a legal contract or agreement.

The MSaaS Provider is responsible for the interoperability and composability between M&S products and solutions. The MSaaS Provider is not responsible for developing M&S products and solutions, and does not always own them.

The MSaaS Provider is also responsible for monitoring and measuring load balancing relevant to the usage of the MSaaS capabilities, and is responsible for billing according to license agreements.

User:

The MSaaS User directly or indirectly consumes MSaaS products and solutions. There are two types of Users that need to be considered: the Operational Users and the Simulation Users.

"Operational Users" indirectly consume MSaaS products and solutions in accordance with meeting operational needs, e.g. training audience in CPX/CAX.

"Simulation Users" directly consume MSaaS products and solutions to provide simulation capabilities and applications to the Operational User, e.g. CPX/CAX operator.

What makes the difference is the direct interaction with simulations and simulators and supporting data and applications. The Operational User consumes only results of simulation, thus he is unaware of the way the M&S Services are realized and delivered to him. The Simulation User directly interacts with the simulation environment and the MSaaS Framework will require new approaches and operational procedures to satisfy the operational community's needs, regardless of the End User's business area (e.g. training, operation planning or support to Concept Development and Experimentation).

To provide more clarification on these different roles, consider a Military Computer Assisted eXercise (CAX), like a Command Post eXercise (CPX).

In this example the Command Post (CP) at the Brigade level is the primary training audience. This audience consists of Commanders and Staff Officers who benefit from using simulated scenarios based on M&S products and solutions (e.g. to have an operational picture, obtain orders, feedback and/or receive events which they need to respond to). This audience (i.e. Operational User) is not responsible for the direct configuration of M&S products and solutions. Training centre personnel (i.e. "Simulation Users") are responsible for directly configuring the scenario aimed at training the Operational User by creating events and using models based on M&S products and solutions available from the Allied MSaaS Framework. Furthermore there could be other users of M&S products and solutions, such as a secondary training audience (e.g. 'role players') who configure and/or interact with constructive simulation tools to provide the behaviour of lower level force units, e.g. squad, platoons. In this instance these are considered to be "Simulation Users."

Supplier:
MSaaS Suppliers develop and provide M&S products and solutions to the Allied MSaaS Framework either via a product procurement or license agreement. These can include large defence contractors, small medium enterprises and academic institutions, in addition to Simulation Users.

Table 1-1: Stakeholders Analysis provides a rough stakeholder analysis

| **Stakeholder Type** | **Motivation** | **Interest** | **Power** |
|---|---|---|---|
| Customer | M&S Support for core business (operational needs, training, SBA etc.);<br>Budget (reduced cost) | Based on benefits | High (Establishes capability requirements, budget) |
| Provider | Business opportunity | High | Medium |
| Operational User | M&S Capability supporting his core business | Low – interested in result, not in means and techniques | Low |

| | | | |
|---|---|---|---|
| Simulation User | Flexibility, easy upgrade, maintenance… | High | Medium |
| Supplier | Business | Based on business opportunity – from low to high | Depends on M&S market, technology capabilities etc. |

**Table 1-1: Stakeholders Analysis**

### 1.2.2 Relationships between Stakeholders and M&S Services

The MSaaS concept requires negotiation between Customers, MSaaS Providers, Suppliers and Users regarding SLAs, licensing agreements and intellectual property.

The MSaaS Stakeholders defined above can be put into relationships with the three types of MSaaS perspectives which were identified during NATO MSG-131:

- MS Software as a service (MS-SaaS);
- MS Platform as a Service (MS-PaaS);
- MS Infrastructure as a Service (MS-IaaS).

The MSaaS Allied Framework supports all three service models which are inherited from the SOA service model, but there are slight differences. In the context of the MSaaS Allied Framework the three service models are defined as:

- **MS-SaaS**[2]: The MSaaS Simulation User consumes M&S products and solutions "as is" from the MSaaS Allied Framework without the need to manage, control or orchestrate the hardware/software infrastructure;
- **MS-PaaS**[3]:

[2] The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

[3] The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages,

  - The MSaaS Simulation User consumes M&S products and solutions from the MSaaS Allied Framework to compose and/or orchestrate M&S products and solutions to create a more complex simulation environment;
  - The MSaaS Provider maintains M&S products and solutions on the MSaaS Allied Framework (e.g. using a cloud infrastructure);

- **MS-IaaS**[4]: The MSaaS Supplier uses processing, storage, networks and other fundamental computing resources from the MSaaS Allied Framework to develop M&S products and solutions.

In the table below the MSaaS stakeholders are put in relation with their own role in each of the Service Model defined.

Table 1-2 describes possible uses of various service models of the MSaaS Ecosystem by roles.

| **Stakeholders** | | **MS-SaaS** | **MS-PaaS** | **MS-IaaS** |
|---|---|---|---|---|
| Customer | | Not applicable | | |
| User | Simulation User | Yes<br>"as it is"<br>Applications | Yes<br>Set of collaborating applications (constructive and virtual simulations, C2SIM translation services etc.) | No |
| | Operational User | "Results-Oriented," reproduced by | "Results Oriented," reproduced by End User or C2Sim | No |

libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

[4] The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

| | | | | |
|---|---|---|---|---|
| | | End User or C2Sim gateway | gateway | |
| Provider | | Provides it to the User | Provides it to the User | Could provide it to Supplier |
| Supplier | | Provides it to Provider (licensed Software) | Provides it to Provider (MSaaS Platform solution) | Uses the infrastructure for its own M&S applications development |

**Table 1-2: MSaaS Ecosystem by roles**

Resuming the CPX CAX example, the end-users operate directly the M&S tools, "as it is" from the MSaaS framework, so it is a MS-SaaS from the end-user standpoint. When the training centre personnel need to configure and compose M&S applications to build a simulated scenario with more complex features, they will be end-users who interact with the MSaaS framework as a PaaS. No end-user will use the MSaaS framework to deploy their own services or develop their own software on a provided software environment, as in the case of a PaaS in the SOA viewpoint.

## 1.3 The OCEAN Project

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/government, non-government agencies) based upon the use of M&S in order to experiment on new concepts and ideas involving the integration of different systems and technologies. Under this initiative the M&S CoE, supported by Leonardo Company is developing a MSaaS cloud-based test bed prototype, the OCEAN project. The OCEAN project offers an embryonic framework made of a combination of hardware, software and services to automate the deployment of M&S tools and applications in a cloud environment.

### The Platform

The proposed platform aims to offer 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 system architecture involves the use of a hybrid cloud inside which you indiscriminately use physical machines, virtual machines and containers

(Figure 1-2). The PaaS solution adopted is OpenStack installed inside a VMware cluster.

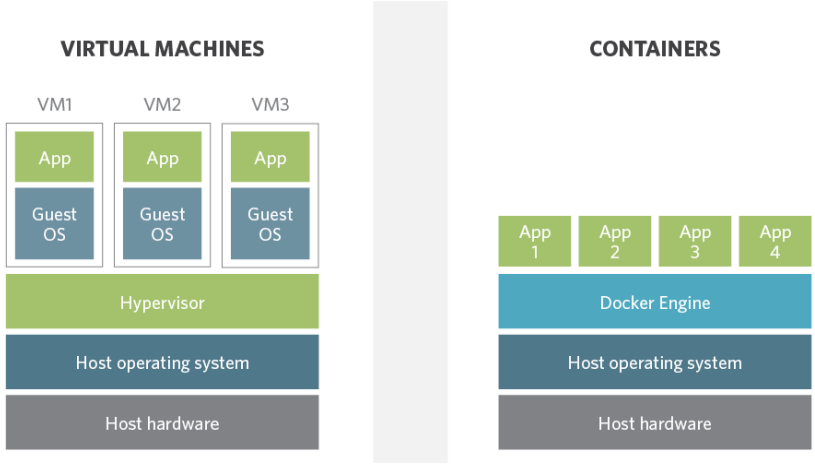



**Figure 1-2: MSaaS System Architecture**

As an open source system, OpenStack enables rapid expansion with external services. An ad hoc service has been developed (inside the OCEAN application stack) for the orchestration of these components: physical and virtual networks; physical and virtual machines; and micro applications (containers).

In this way you can go up the application stack from PaaS to SaaS - a M&S context we call MSaaS. The container management portion is relayed to the VMware Photon Platform solution and the SND (Software Defined Network) part of the virtual network (VXLAN) is implemented by VMware NSX (Figure 1-3).

Due to the structure of a VXLAN, tunnelled traffic can utilize traditional security options, which authenticate and encrypt the traffic. While our existing LAN infrastructure provides the perfect setting, a VLAN can be designated just for VXLAN traffic, providing security with just the servers sending the traffic. The setup ensures that all the end points are authorized on the LAN.

The service developed for MSaaS makes the management of these elements transparent to the users: by accessing a web portal in an agile and simple way, it is possible to create a segregated perimeter within which to insert asset instances (rooms, nodes, networks and software) by selecting them from a catalogue.

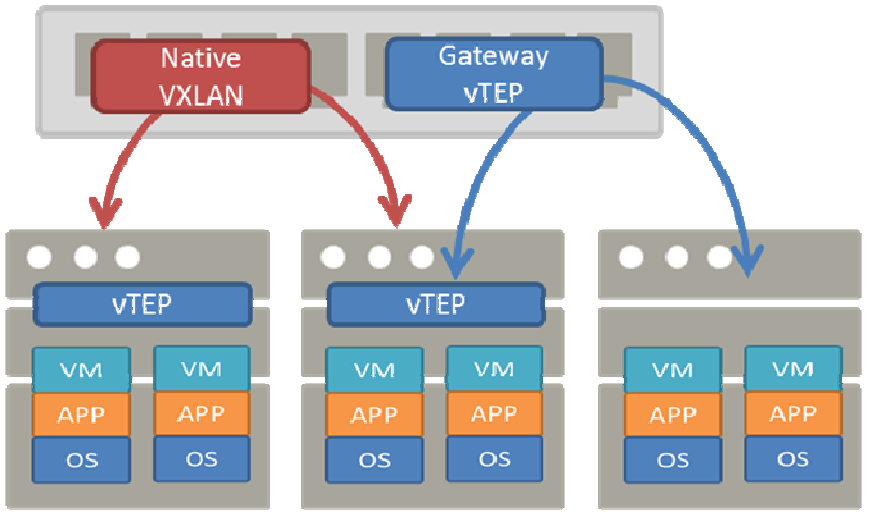



**Figure 1-3: SND Architecture**

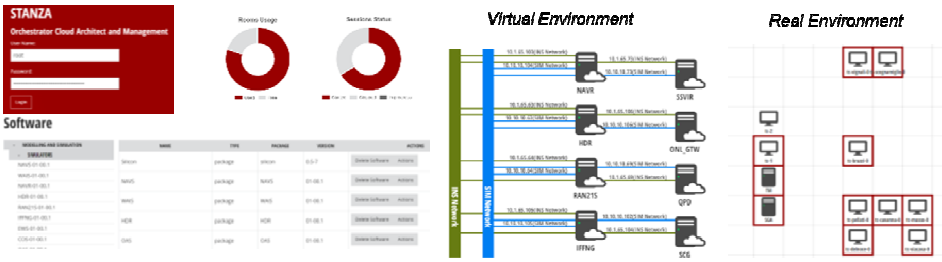



**Figure 1-4: Example of assets networks and rooms management**

After a room is created, it is possible to insert physical nodes inside it, create physical networks to connect physical nodes with virtual nodes, install software, start micro applications connected with virtual networks and so on, all from the OCEAN API. The Web Portal interface uses these APIs to perform the various operations.

OCEAN can then orchestrate all these elements by making the entire infrastructure system transparent and intuitive. A primary advantage of this MSaaS model is that an user with no knowledge of the system is able to use it without difficulty.

## 1.4 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.

NATO M&S CoE and Leonardo are together building a use case of MSaaS based on OCEAN. The aim and complexity of this use case is to put together heterogeneous systems of services, virtual assets, real and physical systems coming both from the M&S and Command and Control (C2) worlds while also being geographically distributed. NATO M&S CoE and Leonardo deploy their assets inside OCEAN, creating an exercise in which a CGF-like (Computer Generated Force) application is stimulating at the same time two different systems: a 3D immersive training environment for communications and a ship combat system simulation.

The following is a short description of the project main components:

- Scenario Generator and Animator (SGA): a CGF application that enables preparation and execution of geo-referenced simulated representing behaviours and interactions among different simulated units and systems.
- Simulation and Validation of Communication (SVC): radio and networks simulator, implementing high fidelity models and reproducing complex data flows and transmissions.
- Equipment Simulators: simulator suite reproducing the on-board equipment for a ship, including navigation systems, radars and other sensors, to stimulate ship's combat management system.
- Combat Management System Simulation: simulation of a ship's combat management system, mainly used for integration activities and training.
- Gateway services: a suite of services able to translate DIS/HLA simulation standards into real system protocols in order to allow the simulation environment to stimulate external assets.
- MORPHEUS system: a 3D immersive system allowing the user to interact with the simulation mainly for training purposes.

All these components are deployed by OCEAN in different ways with different technologies. Real hardware platforms, virtual machine and containers, connect together in a geographically distributed environment to create an exercise room environment where the user can access and operate the different services and applications.

## 1.5 Conclusions

The M&S CoE, Leonardo and other upcoming industrial and academic partners, are joining the project under the OPEN SIMLAB initiative, are designing, developing and implementing an initial MSaaS Prototype called OCEAN. The initial deployment at the M&S CoE of the OCEAN project prototype, provides an embryonic MSaaS services capability that demonstrates the value of MSaaS in relationship to the mentioned use cases.

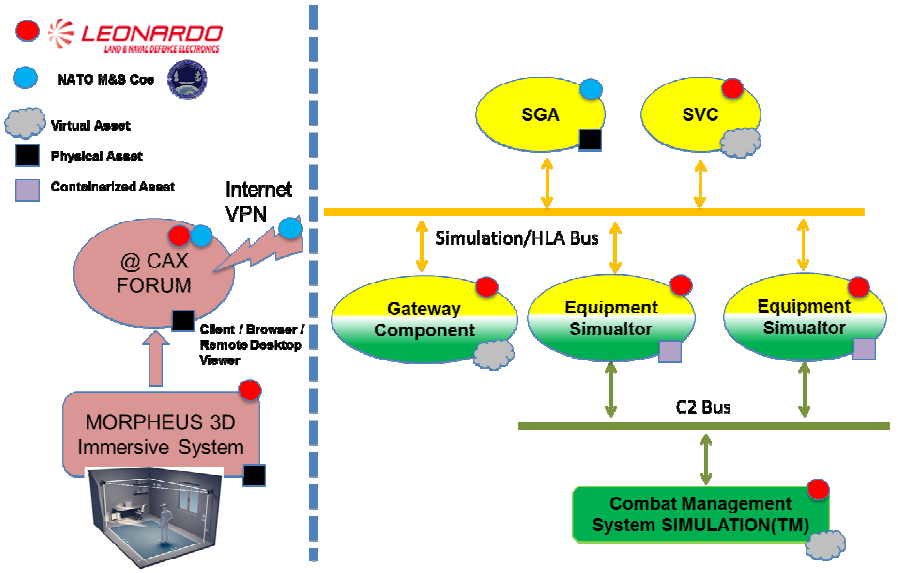



**Figure 1-5: Example of the use case implementation at CAX FORUM 2017**

According to the proposed Stakeholders and M&S services definitions, the OCEAN project is delivering to the NATO M&S CoE a M&S IaaS. With this in place, the M&S CoE could act as a M&S services provider to the MSaaS community of interest, while the Leonardo Company serves as the Supplier. The M&S community of interest that is consuming services could be considered the User and eventually, if they begin producing services, could act as Supplier.

## 1.6 Way Ahead

Further implementation of this capability after the development of mature M&S services, will require a dedicated M&S enclave where users (Simulation and Operational Users) will have access to these services. The M&S enclave is a new concept exploration by the M&S CoE in collaboration with the JFTC, JMSC, and other NATO and national organizations. The M&S enclave concept will require an alignment with the "M&S as a Service" paradigm and the Connected Forces Initiative (CFI), 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. An involvement of NATO NCIA in this exploration is also desirable.

Future plans for the MSaaS include participation in Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) 2017 and presenting a demonstration of the concept at the NATO CAX Forum 2017. The M&S CoE serves as the CWIX M&S Focus Area Lead, and during CWIX 2017 the following capabilities, are going to be experimented: A Scenario Generator and Animator (SGA) as a Service acting as both as consumer of services generating scenarios and as provider of services through a Computer Generated Forces (CGF) service to other Focus Areas like the Operational Command and the Cyber. Following the results of the CAX FORUM demonstration the M&S CoE is going to plan to experiment the OCEAN project, with new M&S service and capabilities, in CWIX 2018.

## 1.7 Acknowledgments

Special thanks go to the M&S CoE's partners, to the Czech Republic University of Defence and to the NMSG 136 members. They made it possible to start to develop and implement this exciting and challenging project.

## 1.8 References

Biagini M, La Grotta M, Corona F, Forconi S, Picollo M, Faillace C, (2016). *NATO MSaaS – A Comprehensive Approach for Military Operational Requirements Development.* Proceedings of the IITSEC 2016

Cayirci E, (2013). *Modeling And Simulation As A Cloud Service: A Survey* . Proceedings of the 2013 Winter Simulation Conference

Cloud Security Alliance (CSA). *2016. The treacherous twelve cloud-computing top threats in 2016.* [ Online]. Available: . https://cloudsecurityalliance.org/download/the-treacherous-twelve-cloud-computing-top-threats-in-2016/. [Accessed June 2016].

Daconta M, (2013). *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].

Department of Defense, Chief Information Officer (2012, July). *Cloud Computing Strategy*. Washington, D.C. VA, USA. Document.

IBM, (2016). *What is cloud computing?*. [Online]. Available: https://www.ibm.com/cloud-computing/what-is-cloud-computing. [Accessed June 2016].

ISO, (2011). ISO/IEC 20000-1:2011. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51986. [Accessed June 2016].

ISO, (2015). *ISO/IEC/IEEE 15288:2015, Systems and software engineering - System life cycle processes*. ISO/IEC JTC 1/SC 7

Mercier, D. (2015). *The new architect of transformation*. The Three Swords Magazine 29/2015, pp. 6-8, Joint Warfare Centre, Stavanger (NOR).

Ministry of Defence, Chief Technology Officer, (2013). *Defence information and communications technology strategy*. UK

NATO ACT CEI. (2013). *NATO Concept Development and Experimentation Handbook*. Norfolk, VA, USA: NATO document.

NATO ACT, (2015, July 15). *2015 Gap Analysis Report on Modelling and Simulation in support of military training*. Norfolk, VA, USA: NATO document.

NATO ACT. (2015). *NATO Urbanization Project.* Retrieved May 2016, from NATO Allied Command Transformation: http://www.act.nato.int/urbanisation

NATO Allied Council. (2012). *NATO Modelling and Simulation Master Plan*. NATO document.

NATO Allied Command Transformation, C4ISR Technology & Human Factors (THF) Branch, (2012, June 15). *C3 Taxonomy baseline 1.0*. NATO document.

NATO Consultation, Command and Control Board, (2007). *NATO Architecture Framework version 3*. NATO document.

NATO NCIA, (2014). *NATO's First Step to the Cloud: Overview and Business Drivers*. NATO document.

NATO Standardization Agency. (2010). Allied Joint Doctrine - AJP 1.0 (D). Brussels, Belgium: NATO document.

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

NATO STO MSG 136. (2017, March 8). Operational Concept Document (OCD) for the Allied Framework for M&S as a Service DRAFT (V. 0.50). NATO document.

NATO STO MSG 136: Modelling and Simulation as a Service. STO CSO - STO activities. (2016). [Online]. Available: http://www.cso.nato.int/activities.aspx?RestrictPanel=5. [Accessed June 2017].

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

Siegfried, R. , Van den Berg, T., Cramp, A., Huiskamp, W. (2014). , *M&S as a Service: Expectations and challenges. In Fall Simulation Interoperability Workshop*, pp. 248-257, Orlando, FL (USA).

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

VMWARE (2015). *A Performance Comparison of Hypervisors* - A performance study [Online]. Available: http://www.vmware.com/pdf/hypervisor_performance.pdf [Accessed June 2016].

Zerger P., Posey B., Henley C. (2012). *The Hands-on Guide: Understanding Hyper-V in Windows Server 2012*.Veeam

# 2. AN AI-ASSISTED CYBER ATTACK DETECTION FRAMEWORK FOR SOFTWARE DEFINED MOBILE NETWORKS[5]

G. Catania, L. Ganga, A. Mursia

Land & Naval Defence Electronics Division - Leonardo Spa

S. Milardo, G. Morabito

DIEEI – Università degli Studi di Catania, Italy

***Abstract***

*In this work we demonstrate how artificial intelligence (AI) can be used to support network managers in detecting and handling cyber-attacks to mobile networks. More specifically, we focus on environments based on a mix of real and simulated networks using the Software Defined Networking (SDN) paradigm. This technology allows for a separation of the data plane from the control plane. The latter is implemented as a software application, called Controller that works in cooperation with the simulation environment. To this purpose the AI engine exploits the information about the network traffic collected by the Controller and uses fuzzy logic to identify anomalies as possible cyber-attacks.*

*When the AI engine detects an anomaly in the traffic flows, an algorithm is executed to identify which is the node that might be responsible of the attack and highlights such node in a graphical user interface. It also sends a warning and suggests a solution to the network manager who is in charge of triggering the countermeasure. A prototype of the proposed solution has been implemented and assessment has been performed exploiting the Cyber Security Simulation Environment (CSSE) developed in the context of the Italian MoD National Plan for Military Research (PNRM).*

## 2.1 Introduction

By clearly separating control and data planes *Software Defined Networking* (SDN) is changing how networks are built and designed in the very fundamentals [13].

[5] This paper originally published as NATO STO MP of the IST 160 working group.

SDN was initially thought to work in infrastructured networks. Recently, however, several solutions have been proposed that extend the SDN approach to networks applying the ad hoc networking paradigm. We call the resulting networks, Software Defined Mobile Networks (SDMNs). Examples of such networks include SDWN [8], FlowSensor [12], and SDN-WISE [9]. Main focus of such solutions was the support of typical functions of such networks such as routing, QoS support, and energy management.

SDMNs are utilized in several tactical scenarios. Recently, we have addressed the problem of security, which is a crucial issue in tactical scenarios, in the case of SDMNs [6]. In fact, note that the SDN paradigm shift implies a radical change in the way security must be dealt with. This involves the need for new tools that should assist cyber and IT operators in reacting promptly during operations and in acquiring the competences required in such contexts.

In this paper we go a step further. In fact, by applying the SDN approach, we define a system element, i.e., the Controller, which receives updates about the status of all network elements. Therefore, the Controller has a global view of the network conditions and of the traffic flowing through it. Such knowledge can be exploited by an *Artificial Intelligence* (AI) engine to detect whether the network is currently under attack and, in case, to determine the type of attack and the corresponding countermeasure. The latter will be suggested to the IT operator who will be the only responsible for triggering it.

Contribution of this paper are twofold. In fact, we introduce a platform that can be used

1. to demonstrate how AI can be used to support IT operators in handling the security of tactical networks using the software defined mobile networking paradigm;
2. to train military professionals in interacting with AI to improve the security of tactical networks based on the software defined mobile networking paradigm.

Note that for both purposes we exploit simulation. In fact, on the one hand simulation is a very valuable tool for validating innovative concepts with small investments. On the other hand, simulation is largely used for training in the military domain and most organizations have valuable simulation infrastructures and facilities (in terms of hardware and software resources).

Accordingly, the rest of this paper is organized as follows. In Section 2 we give an overview of the related work in relevant areas. In Section 3 we describe the proposed platform, while in Section 4 we show preliminary

results of the experimental campaign carried out utilizing our platform. Finally, in Section 5 we draw some concluding remarks.

## 2.2 Background

In this section we provide some background information necessary for the understanding of the rest of the paper. More specifically, in Section 2.1 we focus on the software defined networking (SDN) paradigm and its application to mobile networks with special emphasis on the work carried out to support security in such environments. Then, in Section 2.2 we will focus on the use of machine learning for network management and security support, focusing on artificial neural networks which we will exploit to detect security attacks.

### 2.2.1 Software defined networking for tactical communications

In this paper we focus on tactical networks realized according to the *Software Defined Mobile Networking* (SDMN) paradigm, i.e., we can consider such networks as ad hoc networks that implements the SDN paradigm.

Therefore, nodes of a SDMN are forwarding elements only and the totality of control operations are demanded to a (logically) centralized element running a software program called Controller. To perform efficient and effective control, the Controller exploits information about the current status of the network elements.

Therefore, the SDMN forwarding elements need to collect local information and send it to the Controller through an appropriate, secure communication channel.

Note that the connection between SDMN nodes and the Controller can be achieved in two different ways:

1. There is a long range, low data rate wireless link connecting nodes and Controller directly or connecting both nodes and the Controller to a network infrastructure. Examples of such links include satellite links or links to the base station of a cellular network.
2. Nodes and Controller are connected by means of multi-hop wireless links. In this case an appropriate protocol is needed which allows nodes to send packets to the Controller even if they have not received the relevant information by the Controller. In our work we will consider the protocol introduced in [9].

The way in which packets are forwarded by SDMN nodes depends on the content of a table named “Flow Table”. Like in OpenFlow, each entry in the Flow Table is divided into three sections: rules, action, and statistics.

The rules section specifies the conditions that must be satisfied by the packets to be classified as belonging to a certain flow. Examples of such flows are “all the packets that must be delivered to a given node”, “all the packets generated by a certain node”, “all the packets generated by a given application”, etc.

The action section specifies how the node should behave upon reception of a packet belonging to the corresponding flow. Examples of actions are “forward the packet to a certain node”, “drop the packet with a certain probability”, “modify the packet”, etc. Finally, the statistics section specifies how many times a given Flow Table entry has been used.

Upon receiving a packet a SDMN node browses its Flow Table to verify whether such packet satisfies the rules of a given Flow Table entry. If this is the case, then the node behaves as given in the action section and updates the statistics information. Otherwise, the node encapsulates the packet into a new packet, which is sent to the Controller.

The Controller will take care of delivering such a packet and will send the node a new rule that can be used in the future to deal with packets belonging to the same flow.

Recently, we have demonstrated how security can be handled in SDMNs [6]. More specifically, we have introduced and validated the Cyber Security Simulation Environment (CSSE) which is a platform that provides a simulation environment modelling the impact of cyber attacks and related countermeasures in SDMNs.

In this paper we go further our previous work by enriching the CSSS with artificial intelligence capabilities which support the network manager in taking decisions regarding security in SDMNs.

### 2.2.2 Machine learning for network management and security support

Machine learning can be considered at the base of self-organizing networks.

Accordingly, machine learning and in particular Artificial Neural Networks (ANN) related technologies have been widely used in the past few decades as tools capable of executing network management.

More specifically, *Artificial Neural Networks* (ANN) are a machine learning instrument developed to mimic the behaviour of the human brain. An ANN consists of multiple interconnected nodes, called *neurons*, that resemble a

neural network. Each neuron is connected to other neurons through weighted links and neurons are grouped together into layers. From a functional point of view a neuron contains an *activation function* which returns a value depending on the values provided by the incoming links multiplied by their respective weights. This value is used as input for other neurons and the process is repeated until the last group (layer) of neurons returns the output of the ANN. The process that allows to select the weights of the links of the network is called *training*. For more details on ANN and training algorithms please refer to [5].

There are two kinds of ANN: feed-forward neural network and recurrent neural networks (RNN). In feed-forward networks all the connections between the neurons share the same direction, from one layer to the next, and there are no connections between neurons at the same layer or connection providing inputs from a neuron to another of previous layers. This restriction is removed in recurrent neural networks which, therefore, present a short term memory, as opposed to the long term memory acquired during the training phase.

The main drawback of these ANN is the Vanishing Gradient (VG) problem. RNNs learn the weight by measuring how a small change in the weights will affect the network's output. If a change in the input causes a very small change in the output the network is not able to learn effectively [10].

To solve this issue Long Short Term Memory ANN (LSTM- ANN) were introduced in [10]. These RNNs are able to reduce the VG using some special units called gates that can change the weights or truncate the gradient when needed.

The applications of LSTM are multiple: natural language process, handwriting recognition, and, for what concerns the topic of this paper, time series analysis and prediction [19].

An extensive literature exists on the application of machine learning and ANN to network management and security support [11], therefore we consider only those works which exploits these techniques in the SDN context.

In [1] the authors provided a machine learning based framework to predict the Quality of Experience in SDN. In [16] Particle Swarm Optimisation (PSO) and Genetic Algorithms (GA), are employed to find the best set of inputs that give the maximum performance of an SDN. In [2] it is presented a metheuristic for dynamic optical routing implemented as an application into a software-defined mobile carrier network using machine learning to predict tidal traffic variations.

Machine learning and neural networks have been used to manage network security as well. Relevant examples include the use of Bayesian neural networks to classify Internet traffic [4], the use of machine learning for the detection of network intrusion [17], and the use of machine learning for automatic malware analysis [15].

More recently, artificial intelligence solution running over SDNs have been proposed to improve security as well. For example, in [7] neural networks are utilized to detect DDoS attacks in SDNs, whereas, in [14] it is proposed to train machine learning algorithms on historical network attack data, to predict attack patterns in SDN networks.

### 2.3 Artificial intelligence-Enhanced CSSE

In this section we will present the CSSS platform enriched with AI capabilities assisting the IT operator in managing security in tactical networks.

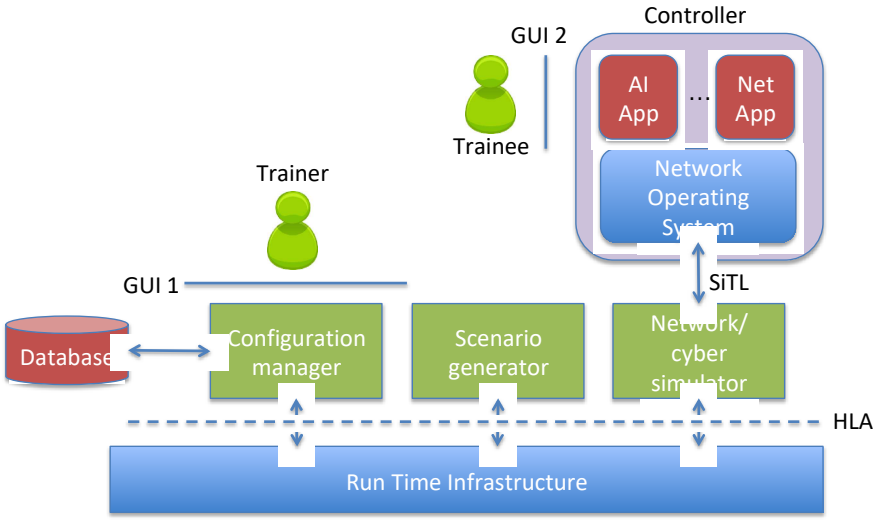



**Figure 2-1: AI-enhanced CSSE platform.**

In Figure 2-1 we represent the architecture of the proposed platform. Major components of the proposed platform are

- The *Configuration Manager*: it enables the interaction between a user (the *Trainer*) who can set and modify dynamically simulation configurations. The Trainer can at any time, decide the type and modality of attacks to be simulated by exploiting an appropriate Graphical User Interface (GUI 1). Exemplary simulation configurations and settings can be stored in a database and can be

loaded when desired. In our platform the Configuration Manager is a proprietary solution developed by Leonardo.

- The *Scenario Generator* components: it generates and manages the simulated scenario (i.e. the movements of troops, vehicles, etc) in a given operation according to the inputs coming from the Configuration Manager. The CGF utilized in our platform is based on the software Stage by Presagis (https://www.presagis.com/en/product/stage/).
- The *Network/cyber Simulator*: it is responsible of simulating the communication elements along with the behaviour of the elements performing the cyber-attacks and the related countermeasures. The behaviour of the network elements depends on the inputs coming from the Configuration Manager as well as the CGF components. Furthermore, since the simulated communication elements apply the SDN paradigm, their behaviour depends on the content of their Flow Tables. Such is decided by an external component called *Controller*. In fact the Controller receives information about the current status of the simulated network and decides the behaviour of the communication elements accordingly. To this purpose the System in the Loop (SiTL) approach is utilized. In our platform we use a packet level network simulator based on the Riverbed Modeler (ex OPNET) software (https://www.riverbed.com/gb/products/steelcentral/opnet.html).
- The *Controller*: it implements the *brain* of the network. In other terms, based on the current status of the network the Controller is responsible of setting the behaviour of the individual communication entities. In general, the Controller consists of the Network Operating System (NOS) and several *network applications*. The Network Operating System receives updates by the communication entities about their status and creates an abstraction of the current state of the overall network which is offered to the network applications. Also, it transforms the high level commands issued by network applications into specific messages sent to the individual network elements. In this way network applications are agnostic towards the technology implemented by the network components. In our platform the NOS is based on an extension of the Open Networking Operating System which we have recently proposed for infrastructureless communication networks [3].

  One of the network applications is the AI engine detecting the attack, identifying the type of attack and proposing a countermeasure to the user (the *Trainee*) by means of an appropriate GUI, that is, GUI 2 in Figure 3-1. We call such network application the AI App. The AI App consists of three major modules:

- The "Measurement module": this is based on ONOS REST APIs which are used to collect information about the current network topology and the amount of traffic traversing each link of the network
- The "Attack detection and classification module": this implements the LSTM- that is trained on historical data to detect anomalies in the network topology and traffic flows. Also, the module implements a classification engine which identifies the type of attack.
- The "Attack countermeasure module": this module exploits the output of the Attack detection and classification module to determine the most appropriate countermeasure to propose to the Trainee. This will be the only responsible on deciding whether to apply such countermeasure. The Attack countermeasure module also implements the interface (GUI 2) for the interactions between the AI App and the Trainee.

Interactions between the Configuration Manager, the Computer Generated Forces, and the Network Simulator are realized in *publish/subscribe* fashion based on the High Level Architecture (HLA) standard [18].

### 2.4 Experimentation

In this section we will present preliminary results of the experimentation we have carried out to validate the AI-enhanced CSSE. More specifically, in Section 4.1 we will describe the experimental scenario along with the types of attacks and countermeasures which we will consider. Then, in Section 4.2 we will describe the artificial neural network (ANN) we have utilized to implement the "Attack detection and classification module" along with the training procedure. Finally, in Section 4.3 we will show the results of our experimental campaign.

#### 2.4.1 Scenario

As shown in Figure 2-2, we simulate $N = 8$ nodes moving in an area of 1 $km^2$. Nodes communicate in wireless multihop manner and apply the SDN paradigm as described in the previous Section 2.1. Each node is based on 802.11g, working at 24 Mbps. The transmission power of each node is $p_{TX}$ = 0.001 W, and the packet reception power threshold is -95dBm. Among the $N$ nodes there is a malicious node, say node $n^*$, which may perform a black hole attack, that is, communicates to the Controller that a certain number of target nodes are its neighbours even if it is not true. In this way large portion of the traffic towards such target nodes will pass through $n^*$, this will not forward the received packets further but will drop them.

Actually, there are several variations of the black hole attack. For example, in some cases the packets will b.e sent to another malicious node which will eventually drop it; in other cases, the packets are just analysed by $n^*$, and then forwarded towards the intended destination.


**Figure 2-2: Simulated scenario**

Several countermeasures have been proposed to address the black hole attack. In our case, the AI module running in the Controller will detect the attack and will try to identify the malicious node(s). Once such objectives are achieved the Controller will inform the network manager that there is the possibility that a black hole attack is ongoing, that the suspected malicious nodes has been identified, and will provide a view of the current topology with an interface which allows to exclude the suspected node from the network. The network manager will use such information to take its own decisions and will take an action accordingly.

Note that after excluding a node from the network, the network manager can re-include it at any time. For, example, this can be done after a software check is performed on the suspected node to verify that the protocol stack has not been violated or, in case, after the correct operations of the node is re-established.

### 2.4.2 Design and training of the artificial neural network (ANN)

As described in the previous Section 3, the *Measurement module* periodically collects the current local status by the network nodes. This is

represented as the number of packets forwarded by a node to other nodes, up to the current period *t*. More specifically, at the *t*-th period the current status for node *i* can be represented by an *N*-tuple, in which the *j*-th the value $v_{ij}[t]$ represents

- the overall number of packets forwarded by node i to node j during periods 1, 2, …, t, if $j \neq i$;
- the overall number of packets forwarded to the upper layers of the protocol stack during periods 1, 2, 3, …, t, if j = i.

Accordingly, at period *t* the status of the overall network can be represented as the *N* x *N* matrix, *V*[*t*], containing the values $v_{ij}[t]$ described above.

Note that in our experimental scenario there are *N*=8 nodes and therefore, matrix *V*[*t*] contains 64 values.

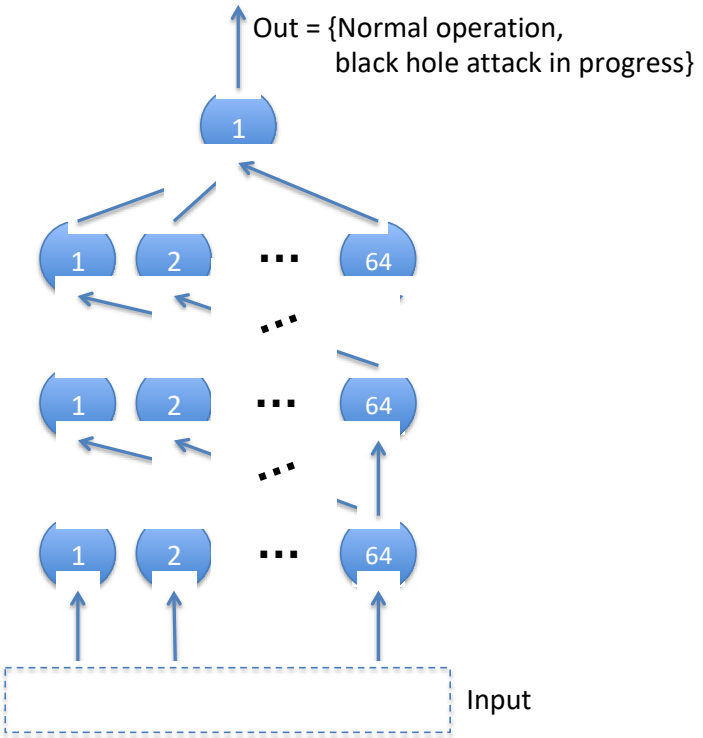



**Figure 2-3: ANN implementing the "Attack detection and classification module".**

Since we focused on a single type of attack, i.e., black hole, the "Attack detection and classification module" is a binary classifier, which we

implemented as an artificial neural network (ANN) consisting of 3 hidden layers each containing 64 neurons, as depicted in the Figure 2-3.

We trained the ANN-classifier with 10000 measures, each labelled as "Normal operation" or "Cyber attack in progress", depending on the simulation configuration and the state of the malicious node. In the considered dataset, half of the measures were taken during normal operations and half during Cyber attacks. In order to train the network, we divided the measures into two subsets, *training* and *test*. The *training* set contains the 75% of the measures and the *test* the remaining 25%. The maximum number of iterations used is 200 and the convergence is reached when the score of the ANN is not increasing by 0.0001 for two consecutive iterations.

### 2.4.3 Results

In order to assess the reliability of the proposed ANN we have evaluated its performance in terms of the three typical performance metrics utilized for binary classifiers:

- **Precision**: it is the ratio between the true positives and the sum of all positives (true plus false positives).
- **Recall**: it is the percentage of positive cases that are detected by the ANN.
- **F1-Score**: it is parameter that averages Precision and Recall.

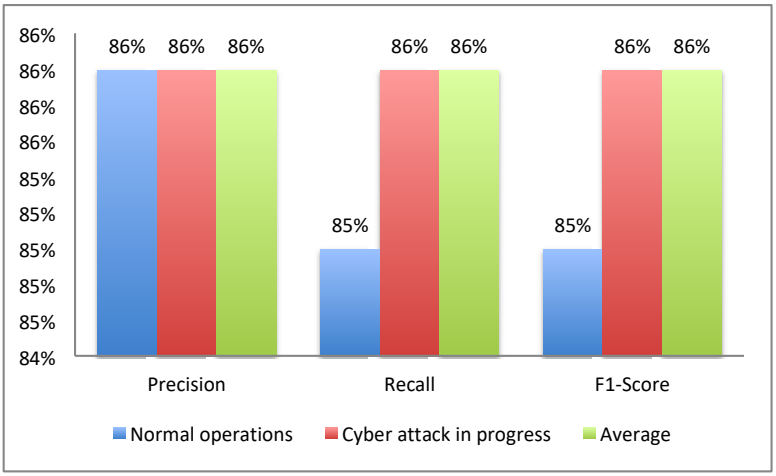



**Figure 2-4: Performance results.**

| | | Reality: Normal operation | Reality: Cyber attacks in progress |
|---|---|---|---|
| Classified as… | Normal operation | 1095 | 182 |
| | Cyber attacks in progress | 173 | 1050 |

**Table 2-1: Results.**

We have evaluated the three above metrics in both the “Normal operations” and the “Cyber attack in progress” cases.

Results are shown in Figure 2-4. More specifically, normal operations were classified correctly 1095 times, whereas attacks were correctly detected 1050 times. Furthermore, there have been 173 false positive and 182 false negatives cases.

In particular, 1095 cases of “Normal operations” and 1050 cases of “Cyber attack in progress” were classified correctly; only 173 cases were classified as false positive and 182 as false negatives.

## 2.5 Conclusions

In this paper we have analysed how artificial intelligence can assist IT operators to detect cyber attacks and trigger the corresponding countermeasures in tactical networks exploiting the software defined networking approach.

An enhancement of the Cyber Security Simulation Environment (CSSE) has been designed and experimental results are presented which assess the feasibility of the overall concept.

This is, however, the first step only in a very promising direction. In fact, it is crucial to determine appropriate tools and methodologies for the training of the AI engines. Also, it is of paramount importance to find the most appropriate interactions modes between military IT professionals and AI tools.

## 2.6 References

[1] T. Abar and S. E. Asmi. Machine Learning based QoE Prediction in SDN networks. Proc. of 13th International Wireless Communications and Mobile Computing Conference (IWCMC). June 2017.

[2] R. Alvizu, S. Troia, G. Maier, and A. Pattavina. Matheuristic with Machine-Learning-Based Prediction for Software-Defined Mobile Metro-Core Networks. Journal of Optical Communications and Networking. Vol. 9, No. 9. September 2017.

[3] A. C. G. Anadiotis, S. Milardo, G. Morabito, and S. Palazzo. Towards Unified Control of Networks of Switches and Sensors through a Network Operating System. IEEE Internet of Things Journal. February 2018.

[4] T. Auld, A. W. Moore, and S. F. Gull. Bayesian neural networks for internet traffic classification. IEEE Transactions on Neural Networks. Vol. 18, No. 1, January 2007.

[5] F. D. Baptista, S. Rodrigues, and F. Morgado-Dias. Performance comparison of ANN training algorithms for classification. Proc. of IEEE International Symposium on Intelligent Signal Processing, 2013.

[6] F. Battiati, G. Catania, L. Ganga, G. Morabito, A. Mursia, A. Viola. CSSS: Cyber Security Simulation Service for Software Defined Tactical Networks. In Proc. of ICOIN 2018. January 2018.

[7] R. Braga, E. Mota, and A. Passito. Lightweight DDoS flooding attack detection using NOX/OpenFlow. In Proc. of Conference on Local Computer Networks, LCN. October 2010.

[8] S. Costanzo, L. Galluccio, G. Morabito, S. Palazzo, Software Defined Wireless Networks: Unbridling SDNs. In Proceedings of the European Workshop on Software Defined Networking, October 2012.

[9] L. Galluccio, S. Milardo, G. Morabito, S. Palazzo. SDN-WISE: Design, prototyping and experimentation of a stateful SDN solution for WIreless SEnsor networks. In Proceedings of IEEE Infocom 2015. May 2015.

[10] K. Greff, R. K. Srivastava, J. Koutn´ık, B. R. Steunebrink, and J. Schmidhuber. LSTM: A Search Space Odyssey," IEEE Transactions on Neural Networks and Learning Systems, Vol. 28, No. 10. March 2017.

[11] P. V. Klaine, M. A. Imran, O. Onireti, and R. D. Souza. A Survey of Machine Learning Techniques Applied to Self Organizing Cellular Networks. IEEE Communications Surveys & Tutorials. 2017.

[12] T. Luo, H. P. Tan, T. Q. S. Quek, Sensor OpenFlow: Enabling Software-Defined Wireless Sensor Networks. IEEE Communication Letters. October 2012.

[13] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. OpenFlow: Enabling Innovation in Campus Networks. White paper. 2008.

[14] S. Nanda, F. Zafari, C. Decusatis, E. Wedaa, and B. Yang. Predicting network attack patterns in SDN using machine learning approach. Proc. of IEEE Conference on Network Function Virtualization and Software Defined Networks. 2017.

[15] K. Rieck, P. Trinius, C. Willems, and T. Holz. Automatic analysis of malware behavior using machine learning. Journal of Computer Security. Vol. 19, No. 4, 2011.

[16] A. Sabeeh, Y. Al-Dunainawi, M. F. Abbod, and H. S. Al-Raweshidy. A hybrid intelligent approach for optimising software-defined networks performance. Proc. of International Conference on Information Communication and Management (ICICM). May 2016.

[17] R. Sommer and V. Paxon. Outside the closed world: On using machine learning for network intrusion detection. In Proc. of IEEE Symposium on Security and Privacy. May 2010.

[18] IEEE 1516–2000 – Standard for Modeling and Simulation High Level Architecture.

[19] LSTM Applications. [Online]. Available: http://people.idsia.ch/ juergen/rnn.html

# 3. DATA FARMING SERVICES IN SUPPORT OF MILITARY DECISION MAKING [6]

Maj Tobias KUHN

NATO Modelling and Simulation Centre of Excellence, Rome (ITA)

Nico DE REUS

TNO, The Hague (NLD)

Maj. Ab DE VOS

Ministry of Defence JIVC/KIXS (NLD)

Lt.Cdr. Bernt ÅKESSON

Finnish Defence Research Agency (FIN)

Gary HORNE

MCR, McLean, VA (USA)

Viktor STRITOF

CZU/ERS (SVN)

LtCol Stephan SEICHTER

Bundeswehr Office for Defence Planning (DEU)

Alexander ZIMMERMANN, Kai PERVÖLZ

Fraunhofer IAIS (DEU)

***Abstract***

*Data Farming is a quantified approach that examines questions in large possibility spaces using modelling and simulation. By harvesting simulation data from many runs set up in a cogent manner, the data farming process evaluates huge amounts of simulation data to draw insights to support military decision making. Data Farming has been codified and methods for actionable decision support have been developed in the MSG-088 and MSG-124 Task Groups. Currently, the new MSG-155 Task Group has*

[6] This paper originally published as NATO STO MP of the IST 160 working group.

*started with plans to make Data Farming accessible and usable by NATO and its partners through the development of Data Farming Services.*

*The decision-maker objective of our first use case is to investigate how various network monitoring and detection systems should be deployed in order to effectively protect critical services from a wide range of malicious cyber activity, under various conditions.*

*In the second use case, simulation output is analyzed to identify the effectiveness of policies in comprehensive military operations.*

*In this paper, we will describe progress to date on the use cases with focus on what we need, how we do it now and how this could be enhanced by informing the potential to combine activities in various domains such as Artificial Intelligence.*

### 3.1 Introduction

Military Decision making is performed at various levels ranging from low level tactical decisions taken at unit level to strategic decisions taken at Corps level. In general, all these levels follow a similar approach that entails understanding the assignment, understanding the environment, designing possible solution directions and Courses Of Action (COAs), comparing COAs and deciding which COA to use in the plan. Several guidelines have been developed for this, like the US Army Military Decision Making Process (MDMP, [1]) and the NATO Comprehensive Operations Directive (NATO COPD, [2]).

Besides deciding about which actions to take, decision making is also used in many other areas. An example is “designing”, where the decision is about selecting the best possible design that optimizes certain criteria. Examples of design decisions in a military context are for instance the selection of a configuration of a communications network in order to optimize the cyber resilience of that network or the optimal design of a military compound in order to optimize its defense possibilities.

Decision making is all about making the right (input) choices that optimize results according to certain criteria. Figure 3-1: The decision making problem in terms of system input and optimization criteria.Figure 3-1 shows the input/output relation that exists between (possibly time dependent) choices for the input to a system (or phenomena) and the criteria that need to be optimized, which usually are some Measure Of Effectiveness (MOE).

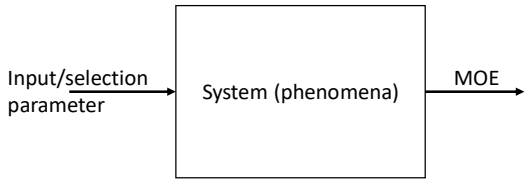



**Figure 3-1: The decision making problem in terms of system input and optimization criteria.**

Finding relations between the parameters that define the choices and the result that the decision maker wants to optimize is of key importance. This search requires insight into the system (or phenomena) that is underlying the input/output behavior. This insight can be obtained in several ways that are shown in Figure 3-2. The two approaches shown are (1) from observations in a live system or phenomena and (2) from observations in an experimental system. The experimental system can either be an operational/live system or a simulation of the represented operational/live system.

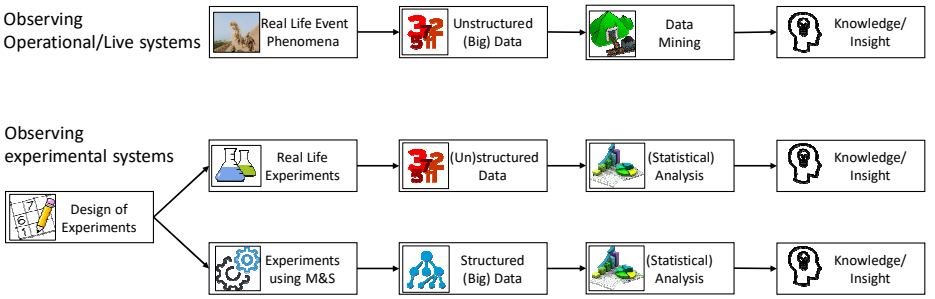



**Figure 3-2: Gaining insight into system behavior, by either observing a live system or doing experimentation.**

When the (usually unstructured) data that is obtained from real life systems is “big”, meaning a lot of data covering a big part of the possibility space (the space spanned by all the possible input choices and corresponding results), we speak of “Big Data”.

When doing experiments a lot of data can be collected. But in this case there are more possibilities to keep the data structured, especially when the data is collected from doing a lot of simulation experiments. In the Design Of Experiments (DOE) it is determined for which input parameters and how many times the experiment is done.

The (Big) (un)structured data, whether obtained from observing operational/live systems or from experimental systems can be used to find patterns in the possibility space, i.e. patterns in the input/output of these

systems. These patterns can be used to infer input/output relations between the possible choices and the results which can be used in decision-making.

When using unstructured data, data mining techniques can be used. Data miners seek valuable information that is hidden in the (big) data using, amongst others, statistical techniques. An important characteristic of data mining is that the miners don't have the control of the data that has been collected, contrary to the case of observing experimental systems. In the latter case the analyst has control over the design of experiment which makes it easier to collect structured data.

M&S which so-far has mainly been used for building training systems, analysis in operational studies and procurement support is currently recognized for its potential use within direct support of military commanders in the decision making process. When M&S for the represented operational/live system is used for generating (big) data that is used for decision-making, we speak of "Data Farming". Within the NATO MSG (Modeling and Simulation Group) a Research Task Group (RTG) called "Data Farming Services (DFS) for Analysis and Simulation-Based Decision Support" was formed and designated MSG-155. In August 2017 the director of the NATO Collaboration Support Office, Alan Shafer mentioned this group in the context of their work being very applicable to IST-160 as quoted in the CSO newsletter of August 2017, …*This group is very much aligned with the STO-160 Theme on Military Decision Making Using the Tools of Big Data and Artificial Intelligence…*

This paper elaborates on how Data Farming can be used for military decision making by discussing the concept and the use cases that are currently under development. It also discusses the possibilities for extending the data farming capabilities with the use of Artificial Intelligence (AI) techniques.

In order to put the Data Farming based Big Data into perspective, section 2 gives some examples of real world observations based Big Data in operational/live systems. Section 3 elaborates on the achievements so far in the Data Farming task groups and especially in the currently active group that deals with Data Farming Services, an approach to bring Data Farming to the operational community. Section 4 discusses the current use cases of the Data Farming Services task group. Section 5 discusses the possibilities of using AI in Data Farming.

### 3.2 Information Extraction and Decision Making from Observing Operational/Live Systems

Observation based big data from operational systems or phenomena uses data collected from the real world based on raw sensor data. Sensors in this

respect should be interpreted as the data collection devices or methods. These can range from real sensors like radar or cameras to internet logging algorithms for social media or administrative applications maintaining event records.

In order to clarify the difference between the use of observations of operational systems and experimental systems (whether live or simulated), in this section two short examples of the big data from observing operational phenomena are given. The examples are: predicting the enemy deployment of IEDs (Improvised Explosive Devices) and the extraction of terrain features from images.

**Counter IED decision making.**

When planning counter IED operations, knowledge about locations where IEDs can be expected is of vital importance. Figure 3-3 shows the global chain of steps that need to be taken.

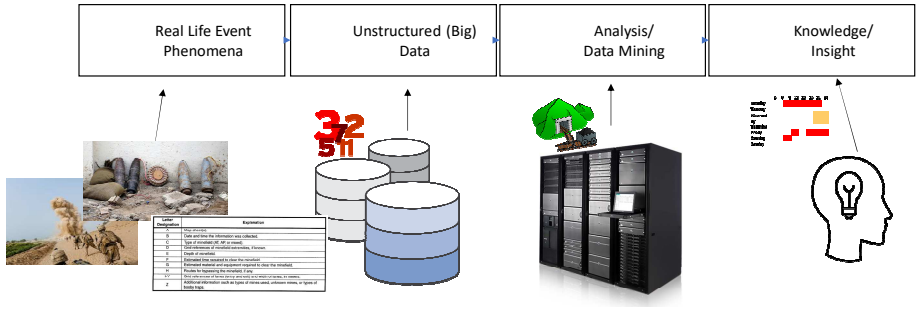



**Figure 3-3: Example of gaining insight into IED phenomena behavior by collecting IED report data..**

In this case, data is collected in the form of historical IED incident reports (containing information about day of week, year, location, specific situation, …) which is searched for patterns in to plan a counter IED operation.

**Targeting decision making.**

When deciding about which objects to target, (satellite) imagery can be used to search an enemy terrain. Figure 3-4 shows the global chain of steps that need to be taken.

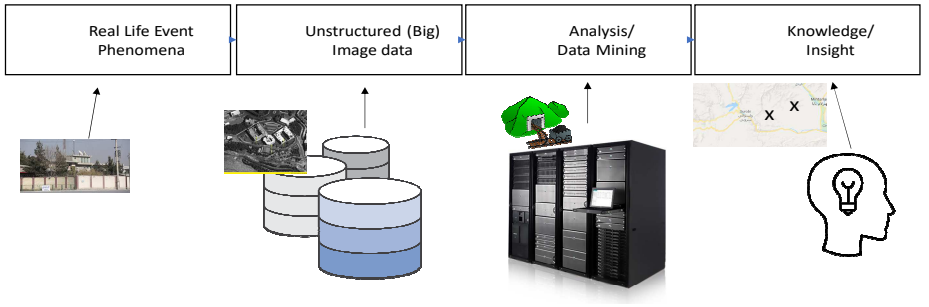



**Figure 3-4: Example of gaining insight into possible target by satellite imagery.**

## 3.3 Data Farming / Simulation Based Experimentation

Data farming is a simulation based experimentation process that has been developed to support decision-makers by answering questions that are not currently addressed. Data farming uses an interdisciplinary approach that includes modelling and simulation, high performance computing, and statistical analysis to examine questions of interest with large number of alternatives. Data farming allows for the examination of uncertain events with numerous possible outcomes and provides the capability of executing enough experiments so that both overall and unexpected results may be captured and examined for insights. Thus data farming provides an unprecedented possibility of mapping the possible consequences of decisions. With this approach, analysis of many different situations can be aggregated enabling ready-to-use decision support. Simulation-based decision support complements operational experience with an objective, reproducible and transparent analysis. This opens up new possibilities by examining thousands of alternative decision factors revealing factors of importance concerning operational outcomes.

The data farming concept has been studied within NATO context in MSG-088 “Data Farming in Support of NATO” [3] and MSG-124 “Developing Actionable Data Farming Decision Support for NATO” [4] and is currently under study within MSG-155 “Data Farming Services (DFS) for Analysis and Simulation-Based Decision Support” [5]. The first study concentrated on the concept, the second one on the use of the concept and the last one on the further usability of the concept through providing a services approach to the users. The following subsections elaborate on these task groups.

### 3.3.1 MSG-088

In 2010, the NATO Research and Technology Organization started the Modeling and Simulation Group “Data Farming in Support of NATO” to assess and document the data farming methodology to be used for decision

support [3]. The work of this group, called MSG-088 codified the data farming methodology and, in particular, documented the six realms of data farming. The group performed the following case study explorations regarding question areas of interest to NATO nations, with the objective of illustrating the power of data farming for decision support.

A *Humanitarian Assistance/Disaster Relief* scenario was developed in MSG-088 for several courses of action where hundreds of alternatives were examined for each course of action. The scenario was a coastal earthquake disaster with embarked medical facilities; the primary objective being to limit the total number of fatalities. A representative set of strategic and operational questions were explored in the data farming process involving the logistical networks, evacuation chains, and distribution of materials. The analysis identified areas where the disaster response could be improved, what bottlenecks were most important, and quantified the benefits of greater ship-to-shore assets.

A *Force Protection* case study was also performed in MSG-088, a data farming experiment with several courses of action and thousands of alternatives in a joint NATO environment scenario. The results demonstrated that it is feasible to answer operational questions for any desired level of detail and identify robust solutions for the given questions. As a conclusion from this case study, it was evident that better understanding of the governing parameters for the problem can provide further and more far-reaching conclusions and recommendations.

MSG-088 finished their work in 2013 which overall showed that the essence of data farming is that it is first and foremost a question-based approach. The group confirmed that in data farming, the basic question repeatedly asked in different forms and in different contexts is: What if? It engages in an iterative process and enables a refinement of questions as well as obtaining answers and insight into the questions. Thus the task group concluded that harnessing the power of data farming is essential to providing support critically needed in answering questions inherent in scenarios NATO should expect to confront in the future as the challenges our forces face become more complex and uncertain.

Data farming uses an iterative approach that is illustrated by the loop of loops in Figure 3-5. The first realm, *rapid prototyping*, works with the second realm, *model development*, iteratively in an experiment definition loop. A rapidly prototyped model provides a starting point in examining the initial questions and the model development regimen supports the model implementation, defining the resolution, scope, and data requirements. The third realm, *design of experiments*, enables the execution of a broad input factor space while keeping the computational requirements within feasible

limits. *High performance computing*, realm four, allows for the execution of the many simulation runs that is both a necessity and a major advantage of data farming. The fifth realm, *analysis and visualization*, involves techniques and tools for examining the large output of data resulting from the data farming experiment. The sixth and final realm, *collaborative processes*, underlies the entire data farming process.

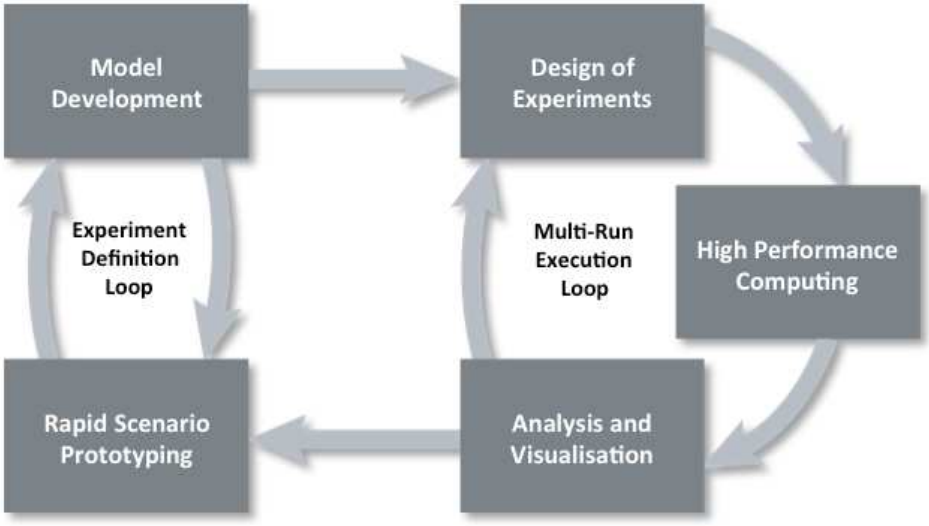



**Figure 3-5: Data Farming Loop of Loops.**

Because the third realm, *design of experiments* (or DoE) will be referred to later when discussing possible uses of AI in Data Farming, we elaborate on it here. DoE is about finding a feasible number of experiments (simulation runs) in terms of computational requirements.

Simulation models may have many inputs or parameters (factors) that can be changed to explore alternatives. A designed experiment is a carefully chosen set of combinations of these inputs, called design points, at which the simulation model will be run. Changing the factors all at once limits your insights. It will allow you to see whether or not this changes the responses, but you will not be able to tell why the changes occur. For example, if mission effectiveness improves when you equip a squad with better sensors and better weapons, you will not know whether it's the weapon or the sensor that has the most impact. Changing the factors one at a time also limits your insights. If the squad gets a very small improvement from a better weapon, a very small improvement from a better sensor, but a large improvement from both, you will not be able to identify this interaction (or synergistic effect) if the experimental design does not involve factors for both the weapon and the sensor. Changing the factors in

a brute force way, by looking at all possible combinations, is impractical and most of the time impossible, except for extremely simplistic simulations with only a few factors. Suppose for instance that you have 100 sensors, each of which can be turned on or off, there are $2^{100}$ (which is approximately $10^{30}$) possible sensor configurations. If every configuration was simulated in an experiment, then even with the world's fastest supercomputers this would take more time than the age of the universe to calculate.

DoE helps overcome the curse of dimensionality, while letting you achieve a broad variety of insights about your simulation model's performance. It provides smarter ways of setting up the experiment that facilitate follow-on analysis and visualization of results in a reasonable amount of time. The review paper by Kleijnen et al. [6] presents a portfolio of existing DoE methods that can be used in simulation experiments. In this review, criteria for evaluating designs are listed and explained, and a design toolkit for simulation experiments is provided.

### 3.3.2 MSG-124

The core objective of MSG-124 "Developing Actionable Data Farming Decision Support for NATO" [4] was to apply actionable Data Farming that could contribute to the development of improved decision making of relevance to NATO forces.

The task group applied Data Farming (DF) capabilities within NATO and Partners that could contribute to the development of improved decision support to NATO forces. MSG-124 took the results of concept explorations and assessments of possible Courses of Actions (CoA) in specific question areas to recommend and demonstrate a way forward in NATO contexts where M&S methods in concert with Data Farming are useful tools in capturing the possibilities. MSG-124 considered the application areas relevant to NATO: Operation Planning and Cyber Defense.

The Operation Planning Syndicate addressed the question on how to provide actionable support to decision makers in operation planning. The Data Farming Tool for Operation Planning (DFTOP) was developed to support decision makers and analysts. Initial validation efforts have concluded that DFTOP meets the need of the military planner, and successfully brings Data Farming into the actionable decision support domain.

The main goal of the Cyber Defense Syndicate was to explore possible scenarios through Data Farming that could facilitate the understanding of some aspects of cyber defense. The syndicate members developed the Data-

farmable Agent-based Cyber Defense Assessment Model (DACDAM) to support decision-making.

The overall conclusion and recommendation to military leaders was that Data Farming is feasible for NATO and nations, and should be used as a methodology for actionable decision support in operation planning and cyber defense.

### 3.3.3 MSG-155

The previous task groups concentrated on the Data Farming concept and military usefulness. This MSG-155 task group [5] aims at bringing the concept a step closer to the user by decomposing the concept into services. The service concept is called DFS (Data Faming Services). This service oriented approach which was inspired by the Modelling & Simulation as a Service (MSaaS) concept, allows easier use and governance for the user and developer of Data Farming solutions. MSG-155 aims at defining and developing services and demonstrating these by means of use-cases. This section elaborates on the architecture of the service approach.

Using the Data Farming loop of loops (Figure 3-5), first the following structure was derived for the services and related repositories.

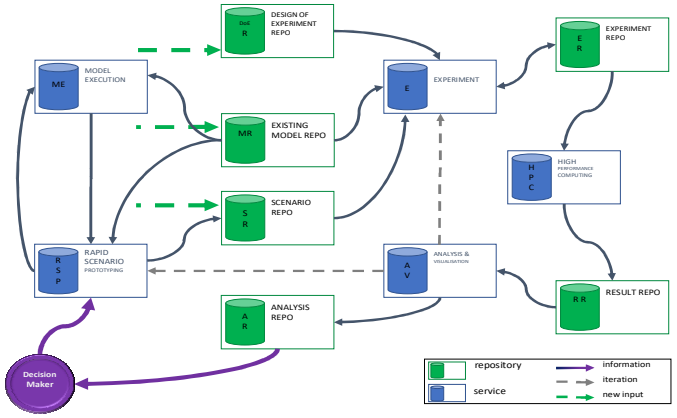



**Figure 3-6: Relations between Data Farming Services and related repositories.**

The architecture of the Data Farming Services (DFS) is being developed in two main steps. First, a common business object model (BOM) is developed based on the contents of the MSG-088 Final Report which codified the methodology of Data Farming in support of NATO. Second, based on this BOM services are defined which cover the capabilities of all Data Farming realms.

There are three kinds of services in DFS:

- *Repository* services which handle the management of the business objects like accessing, storing and versioning.
- *Business services* (stateless) which use the business objects by conducting automated actions in order to support specific Data Farming capabilities.
- *Cross sectional support services* like Configuration and Security in order to handle, support and enforce the structure and usage of DFS.

All services are implemented as REST-Web Services. Communication will be secured by HTTPS and OAuth2. A web application, the DFS-Portal, is implemented using modern web technologies. It acts as central starting point for all DFS actions and supports the user in business object handling as well as performing Data Farming processes.

Nevertheless, all services can be used directly by accessing their corresponding service endpoint programmatically which, for example, supports the use of specialized desktop applications for specialized analyses. The DFS-Portal is meant for supporting the user in accessing the services and conduct single service actions or more complex workflows like creating and executing a DF-Study. An overview of the architecture is depicted in Figure 3-7.

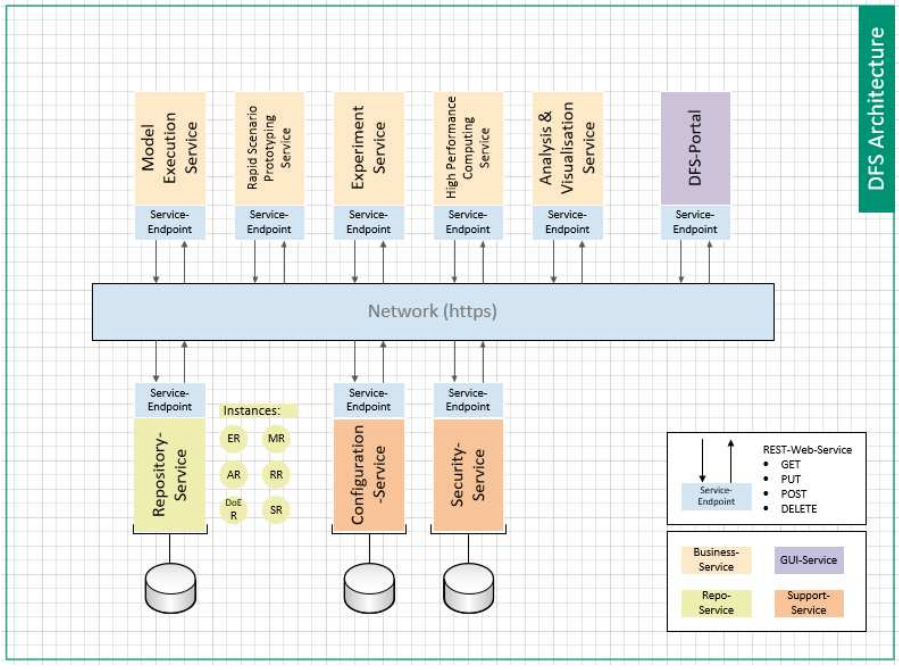



**Figure 3-7: Overview of the DFS architecture.**

## 3.4 MSG-155 USE-CASES

The following subsections describe the current two use-cases currently being worked on in MSG-155.

### 3.4.1 Cyber Defense use case: Optimal Placement of Sensors in a Computer Network

The decision-maker objective of this USA-Finland led use case is to investigate how various network monitoring and detection systems should be deployed in order to effectively protect critical services from a wide range of malicious cyber activities, under various conditions. For this purpose, an agent-based simulation model will be used to analyze different solutions and find optimal configurations with regard to some user-defined measures of effectiveness or desired end state.

Additionally, the methodology objective is to demonstrate the Data Farming Services framework and provide requirements for the core services.

#### 3.4.1.1 Decision maker's question

The question of interest in this use-case is: how should organizations invest their resources to maximize their ability to defend themselves against cyberattacks? More specifically, how should various network monitoring and detection systems be deployed in order to effectively protect critical services from cyberattacks?

#### 3.4.1.2 The Cyber use-case model

The Data-farmable Agent-based Cyber Defense Assessment Model (DACDAM) was developed in the Cyber Defense Syndicate of MSG-124 [4], [7]. The DACDAM model is composed of three primary elements: the network, the system administrator and the attackers. In this use case, additional features will be added to the DACDAM model. Figure 3-8 shows a view on DACDAM's user interface.

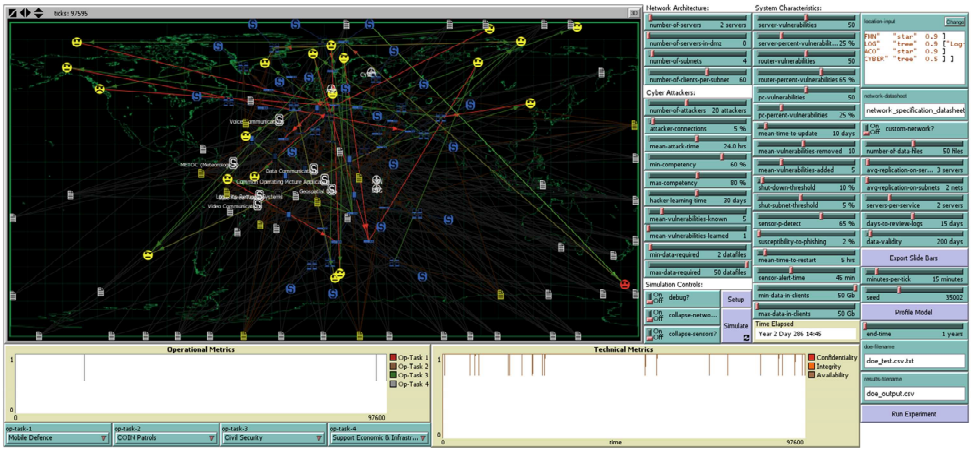



**Figure 3-8: DACDAM GUI**

The network model includes a number of network elements (routers, servers, subnets, clients) and sensors to detect cyber attackers. The network administrator is currently modelled employing a simple algorithm using the shutdown thresholds specified and the alarms communicated by the sensors. The system administrator monitors the sensor alarms and either shuts down affected subnets, or the entire network depending on the number of alarms and the threshold parameters. The cyber attacker model is based on a series of tasks that hackers follow and transitions between the states. Each hacker follows a different strategy by having different probabilities for transitioning between states.

The model includes networked services (applications) and data files associated with the services. These can be denied or compromised by attackers. Additionally, services can be mapped to operational tasks, which can be further mapped to operations. This provides one way of assessing the impact of cyber-attacks.

The initial version of DACDAM, version 0, is implemented in the NetLogo framework, but it is currently being migrated to Python.

The current general sensor model will be extended to distinguish between different types of sensors with different properties.

### 3.4.1.3 Model Input/Output

*Inputs include:*

- Network characteristics, e.g. number of attackers, number of vulnerabilities in the network elements, mean time to update.

- Network topology. The network topology can be provided by the user or randomly generated based on a few parameters.

*Outputs include:*

- Number of attackers sensed.
- Confidentiality, Integrity and Availability metrics (CIA) of network services.
- Number of compromised data files.

### 3.4.2 COSMOS use-case: Comprehensive Operations Support with Modelling and Simulation

Modern conflict is not only fought on the physical battlefield but also engages actors in the information and human landscape. This often takes place in a comprehensive environment, where not only adversaries are active but also other players, like the population or NGOs. Military interventions aim to influence undesirable dynamics to create a more desirable state of the world. The military has to deal with the fact that the desired end state has more than only military aspects, amongst others there are also political and social aspects involved. A difficult task for decision makers lies in understanding the interactions between actors and factors that shape the conflict and how these actors and factors can be influenced, especially since a lot of uncertainty is involved. Modelling and simulation (M&S) methods that aim to describe and understand the dynamic behavior of complex systems could serve as a capability to structure information and derive insights on the problem and possible interventions. These M&S methods should take into consideration the inherent uncertainties that are involved. The users of the proposed M&S approach are intelligence analysts and operational analysts that serve the commander in making his decisions at the operational level [8].

Additionally, the methodology objective is to demonstrate the Data Farming Services framework and provide requirements for the core services.

#### 3.4.2.1 Decision maker question

The comprehensive operation in this case is about a region with sub-regions where the population consists of two ethnic groups. One group is original and the other has the same ethnicity as the neighboring country. Both groups are historically poorly integrated and one reason is language barriers. Social, economic and identity grievances have recently been growing in the underprivileged non-original ethnic population which has led to a separatist movement. Some terrorist attacks have already taken place. A Brigade sized

group is present in the area and is tasked to stabilize the area, in collaboration with the local government and NGOs.

The question of interest in this use-case is: what is the best policy to follow in this comprehensive operation, given the uncertainty about the environment? A policy is considered good if it results in good MOEs for all possible states the situation can be in and given the inherent uncertainty. In other words, good policies are robust policies. The analysis requires looking into the relation between the policies and the MOEs under uncertainties and taking into account the different geographical locations that are involved. The decision maker should be supplied with higher level information by the analyst about the strengths and weaknesses of a number of policies and analysis, and visualization should help the analyst in formulating this information.

#### 3.4.2.2 The COSMOS use-case model

The overall model from this use-case is a combination of linked entity based System Dynamics (SD) models. Amongst others, for every geographic sub-region an SD model has been assembled as well. These models have been linked for aspects that influence the state of the neighboring sub-region's models. For building the sub-region entity SD models, a classic separatist model from literature was used which has been adopted to the specific scenario/environment. Figure 3-9 shows one sub-region SD model where the structure of the generic separatist model can clearly be seen. The influencing factors are amongst others radicalization, polarization, inequality and perception of the problem. Besides these "resilience capitals" have been defined which contain aspects like economic capital and social capital. The figure also shows some (aggressive) interventions (policies) and where these enter the model.

Because the uncertainty involved in the modelling of comprehensive operations is substantial, this uncertainty has to be dealt with in generating the data farming results. This work is done by parameterizing the model and defining a (large) number of sets of plausible (combinations of) parameters. Large numbers of plausible futures are then generated for each chosen policy. This differentiates data farming with these (uncertain) models with variation in large sets of possible parameters and usually only a handful of policies or combinations of policies from data farming use-cases where the large number of variations are in the decision space and not in the uncertainty space.

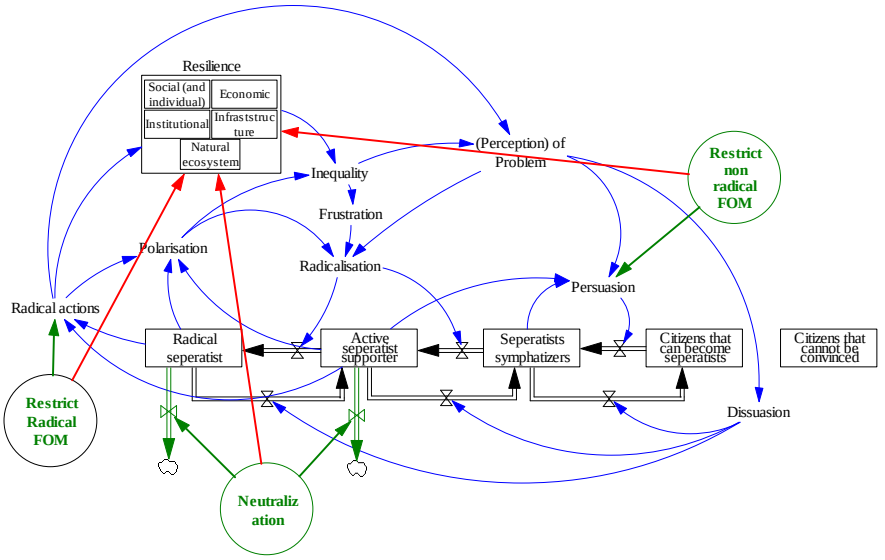



**Figure 3-9: Sub-region model (based on generic separatist model) with indications for some aggressive interventions.**

Figure 3-10 shows a visualization of the sub-regions from the scenario.

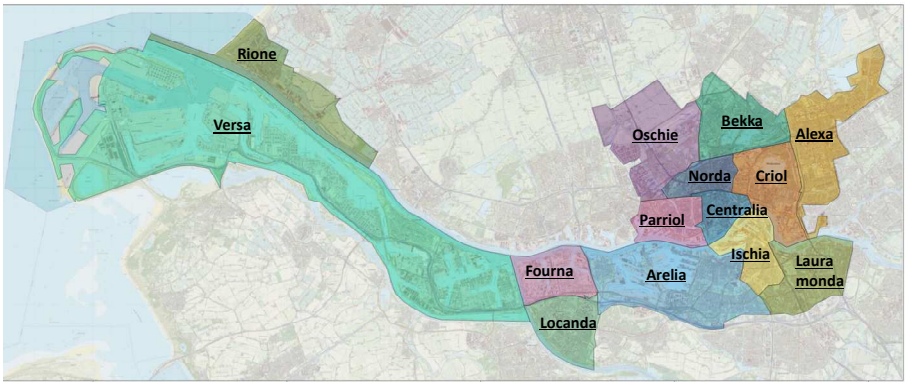



**Figure 3-10: Sub-regions of the overall scenario.**

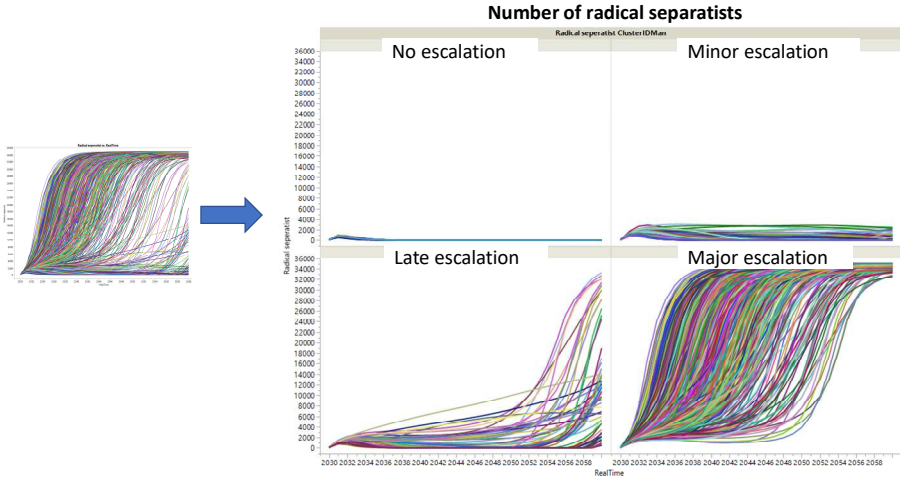



**Figure 3-11: Clustering of scenario output of one sub-region model for one policy and varied uncertainty.**

Figure 3-11 shows one output (# radical separatists over time) for one sub-region for all plausible futures resulting from the variation in the uncertain parameters. One method to analyze this output is to search for clusters of similar behavior (in this case: no escalation, minor escalation, late escalation and major escalation) and look in the input space where these behaviors originated.

### 3.4.2.3 Input/output

The input/output shown below is purely illustrative and not complete.

*Inputs include:*

- Policies
  - Aggressive
    - Restrict Radical Freedom Of Movement.
    - Restrict Non Radical Freedom Of Movement.
    - Neutralization of separatists or separatist supporters.
  - Social influence
    - Appease Blue/Red sides.
    - Reduction of problem visibility.
  - Mix Aggressive / social influence.

- Combination of the above.

These policies can be static or time dependent.

- Uncertain parameters.
  - These are a set of various model parameters. An example is the radicalization dependent factor that influences the rate by which separatist sympathizers become active separatist supporters.

*Outputs include:*

- Average capital
- Area capital damage
- Number of radicals
- Radical actions/area
- Separatist support
- Perceived inequality
- Polarisation

### 3.5 AI in data farming

Previous sections have shown the data farming process steps. This section elaborates on the possibilities of Artificial Intelligence (AI) techniques to enhance the Data Farming process. The list is presented along the Data Farming realms.

**Model development / Rapid scenario prototyping**

- Modelling Blue/Red strategies and using these in simulations. In war games, the enemy response (and consequently blue response) can be learned by agents by observing how humans play. This way they can learn from realistic experience. In an earlier Data Farming experiment [9], a red team played many red Course of Action (COA) manually and used a Data Farming toolset in an attempt to augment current operational planning cells in the areas of rapid COA development and analysis. One of the conclusions was to explore automation of this manual process. The current developments in machine learning techniques (for example reinforcement learning) seem to be able to facilitate just that.
- Finding COAs using Evolutionary Algorithms. Although a different type of technology, Evolutionary Algorithms can be used for optimizing military Courses of Action, this is described in [10].

**Design of Experiments (DoE)**:

- Creation of initial DoEs. A rule-based, expert system using symbolic AI is envisioned that could (help) select DoEs based on problem description.
- DoE adaptation based on output results, also called adapted sensitivity analysis. DoEs can be iteratively enhanced by analyzing the output space resulting from a particular DoE and searching for areas of interest in the output space which can be enhanced by using AI techniques.

**Analysis & Visualization**

- Analysis support by finding input/output patterns. AI techniques to identify relations between desired output (indicated by human operators) to the input space. Thus finding the commonalities of input values that lead to desirable outcomes This can help the analyst in finding desirable regions in the output space and draw conclusions about inputs that caused these findings.

**General data farming**

- Data Farming assistant. In [6] a recommendation is provided for DoEs according to the number of input factors and output space complexity. It is imaginable that this can be done for the other data farming realms and a rule based system could be built to help in defining the set-up of data farming experiments. Building a taxonomy for characterizing data farming experiments could help in this.
- AI supported meta modelling. When simulations are extensive and time consuming, metamodeling can help to overcome the computational burden. A metamodel can simply be defined as a model of a simulation model. Metamodels are also known as response surfaces, surrogates, emulators, and auxiliary models. Since the simulation itself is a model of some real-world system, process or entity, it takes inputs as the real-world system, acts as a black-box function, and finds the outputs as modeled. A metamodel is the approximation of this black-box function, i.e., it finds an approximation of the simulation output with less computation time. Machine learning techniques (like Neural Networks) are a viable solution for that case.

**Use case specific possibilities**

Cyber use-case:

- Intrusion detection/prevention systems and security information and event management systems analyzing network traffic and security event logs that make use of AI technology already exist. These systems assist network administrators in monitoring and analysis. These systems can detect anomalies and use both supervised and unsupervised machine learning techniques. So, although the inclusion of simulation models of these devices is not directly supporting the data farming process itself, using models of these AI systems is supportive of the modelling phase.

COSMOS use-case:

- Finding robust policies. This idea is a variation of "modelling blue/red strategies" mentioned under the "model development" realm but explicitly taking into account uncertainty. This search would also help in investigating which parts of the model or which parameters are responsible for a policy being robust and "good".
- Tipping point analysis. Typically in the type of nonlinear differential equations that are used in modelling the three landscapes (Physical, Information and Human landscape) there can be scenarios with so-called "tipping points" which are the critical points in an evolving situation that leads to a new and irreversible development. Predicting these tipping points amounts to finding patterns in the system behavior leading up to such a tipping point. It is imaginable that machine learning techniques could help in this prediction.
- Uncertainty reduction. Reducing the uncertainty that exist about model parameters would help in finding better, more valid models. AI techniques could help to steer the data collection process by prescribing which real life phenomena should be observed in order to reduce the uncertainty that exists in some model parameters.

### 3.6 Recommendations and Way Ahead

A Data Farming perspective Roadmap of AI developments for Data Farming should be developed. We recommend the exploration of the AI related ideas that were discussed in the previous section. The priority from the perspective of MSG-155 should be in the following order:

- Scenario development
- DoE
- Analysis support

There are many ideas for enhancing the Data Farming Services concept (called Data Farming 2.0) and the use of AI is seen as one of them. Because

the Data Farming Services study group (MSG-155) is still welcoming nations to participate and bring in their own use-cases it will be especially appreciated if the use-cases currently under study within MSG-155 could be enhanced by an AI related use case.

## 3.7 REFERENCES

[1] US Army, "Field Manual 101-5: Staff Organization and Operations," Department of the Army, 1997.

[2] Supreme Headquarters Allied Powers Europe (SHAPE), "Allied Command Operations Comprehensive Operations Planning Directive COPD interim v2.0," NATO, 2013.

[3] NATO, "STO-TR-MSG-088: Data Farming in Support of NATO," NATO Science and Technology Organization, 2010.

[4] NATO, "STO-TR-MSG124: Developing Actionable Data Farming Decision Support for NATO, Pre-release," NATO Science and Technology Organization, 2018.

[5] NATO, "Technical Activity Proposal MSG-155: Data Farming Services (DFS) For Analysis And Simulation-based Decision Support", NATO Science and Technology Organization, 2017

[6] J.P.C. Kleijnen and W.C.M.V. Beers, (2005). Robustness of Kriging when interpolating random simulation with heterogeneous variances: Some experiments, *European Journal of Operations Research,* 165(3), pp. 826-834. doi: 10.1016/j.ejor.2003.09.037.

[7] G. E. Horne and S. Balestrini Robinson, "Data Farming and Quantitative Analysis of Cyber Defense Technologies and Measures, paper No. 33," in *MODSIM World*, 2016.

[8] B.M.J. Keijser, G.A. Veldhuis, N.M. de Reus (TNO) "M&S in support of the operations process: Challenges and a novel implementation", NATO Operations Research and Analysis Conference 2017

[9] Project Albert International Workshop 10, Team 1 Outbrief, Use of Project Albert Tools for Course of Action Development, Stockholm, May 2005.

[10] S. Haider and A.H. Levis (George Mason University) "Courses of Action for Effects based Operations using Evolutionary Algorithms", Proc. SPIE Defense & Security Symposium, Orlando, FL, April 2006

# Part II

# REPORTS

# 4. CRISIS MANAGEMENT EXERCISE (CMX) 2018 - SUPPORT TO THE NATO DEFENCE COLLEGE – NRCC.

Lt.Col. A. Russo

NATO Modelling and Simulation Centre of Excellence, Rome (ITA)

## 4.1 Introduction

The NATO Modelling and Simulation Centre of Excellence (M&S COE), in line with its mission[7], enthusiastically supported the NATO Defence College (NDC) - NATO Regional Cooperation Course (NRCC) during the Crisis Management Exercise (CMX), executed in April 2018. Subject Matter Expertise and best practice from the NATO M&S COE were made available and resulted instrumental to develop and illustrate the digitalized scenario model used by tutors and students during CMX.

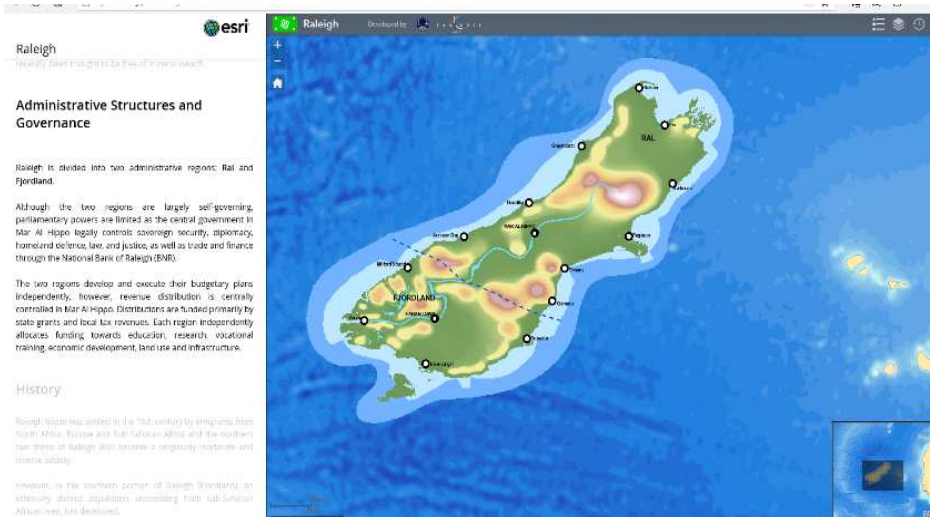



**Figure 4-1**

[7] NATO COE Catalogue ed. 2018 pag. 52 - http://www.act.nato.int/images/stories/structure/coe_catalogue_2018a.pdf [Accessed 23 May 2018]

The NRCC[8] is the Alliance's major educational outreach to Mediterranean Dialogue (MD) and Istanbul Cooperation Initiative (ICI) countries and partners, from the broader region of the Middle East. The aim of the course is to link issues of concern both to MD and ICI nations and to NATO, in order to develop mutual understanding and networking among participants.

The latest NRCC[9] held in February – April 2018 has seen participants form 18 Countries including high ranks military officers, civilian officials and diplomats from the Ministry of Defence, Ministry of Foreign Affairs, and other ministries or administrations concerned with strategic security issues.

The final week of the NRCC was dedicated to the CMX, where participants had the opportunity to apply the knowledge they have gained during the course.

### 4.2 NATO Modelling and Simulation COE - Effective Solution Development

To support the NRCC CMX conducted at the NATO Defence College, the NATO M&S COE along with industrial support, contracted by NDC, have developed a geo-referenced digitalized scenario model with visual information drawn out from the hard copy of the CMX exercise scenario, which comprises:

- Easy to use descriptive narrative scenario sections (figure 1) complemented by geographic maps as well as multimedia contents
- Multi informative layers, such as:
    - Basemaps
        - Global basemap with borders
        - Island morphology terrain basemap
    - Climate
        - desertification area
    - Crime map
        - terrorist potentially dominated area
    - Ethnic groups
    - Places

[8] http://www.ndc.nato.int/education/courses.php?icode=10 [Accessed 23 May 2018]

[9] http://www.ndc.nato.int/news/news.php?icode=1164 [Accessed 23 May 2018]

    - Cities
    - Military bases
    - Oil rig
    - Power plant
    - Refugee camps
    - Dam
    - Places area (disputed area, lithium deposits, oil rigging area, resort, training area)
  - Regions
  - Population distribution
    - Population distribution Annotation (Percentage Label)
    - Total Population in the cities
- Widgets and element of interaction, such as:
  - Layers List
  - Legend
  - Time Slider (timeline feature)

The primary aim of the digitalized exercise scenario was to increase realism, facilitate complex strategic scenario understanding and decision-making processes. Students were required to analyse an initial situation that called for a humanitarian intervention and the establishment of a safe and secure environment. Using comprehensive approach students were stimulated to formulate options/proposals to key-leaders to achieve security and stability.

It is worth mentioning that developed solution, aiming at creating an easy to use interactive platform, evolved around the execution of different work packages, which comprised:

- scenario analysis
- capture of relevant information
- model development
- digitalization of contents, maps and multimedia contents

Additionally, to render the tool usable, other important tasks were fulfilled, such as:

- server and connectivity configuration
- accounts issue to the mentors and students

- training sessions to all the stakeholders to familiarize with the tool
- model live test using internet connection and commercial tablets / computers
- support the live execution phase of the exercise

Among all the activities carried out, Model Development, as an essential part of the entire process, required non-common professional expertise.

To be consistent with the NDC requirement, most significant information were represented in multi-thematic-layers in the model. This method streamlined student's crisis management experiences. Scenario information package encompassed social, political, demographic, economic and military aspects. This approach enabled extensive knowledge of the environment by exploiting state of art technology and using the so-called "Geographic Approach[10]".

The methodology used for this activity came out from another important solution the NATO M&S COE developed in support of a NATO major project called Urbanization Project (UP). In particular, the NATO M&S COE created a digital mega city model using comprehensive approach and PMESII layers structure to facilitate Concept Development Process and validate the Capstone Concept on "Joint Military Operations in an Urban Environment" by the end of 2018. This Concept will be a foundation for follow-on capability development such as functional or operational concepts and a NATO Urban Doctrine.

Leveraging UP framework was key to the NDC CMX supporting tool development.

In general terms, digitalized scenario model provides significant benefits, such as:

- real-time learning experience by exploring informative and geographic data
- greater retention of learned material
- improved interaction with the scenario in the fields of political, military, economic and social implications
- replacement of paper and manual processes

[10] http://www.esri.com/news/arcnews/fall09articles/what-is-geographic.html [accessed 30 May 2018]

- cost-saving
- re-usability

Finally, the model was conveniently used by course Members and Tutors. It introduced an advanced and more interactive way to support CMX during the NRCC.

### 4.3 Conclusions

The NATO M&S COE offers a favorable ground for development of effective solutions to support NATO education and training initiatives. Since its establishment, the NATO M&S COE has needed to keep at pace with the increased interest in using Modelling and Simulation technologies as a key enabler in different areas of interest within the Allied framework. In this respect, cooperation between the NATO M&S COE and the NDC represents a good example of synergic effort among different Allied Entities to work together effectively despite differences in their missions. Properly managing previous experiences helped to avoid duplication of efforts with cost saving benefits. In this respect, effective use and re-use of Modelling and Simulation best practices in support of NATO entities and Nations remains top priority for the NATO M&S COE. In the near future, the NATO M&S COE and the NDC have agreed to increase the level of mutual collaboration and to use digitalized scenario model approach to support other academic courses.

# 5. NATO M&S COE COURSES: NOVEMBER 2017 – JUNE 2018 STATISTICS

CWO Felice D'Aiello

NATO Modelling and Simulation Centre of Excellence, Rome (ITA)

## 5.1 NATO CAX Specialist Course

The Course was designed and developed by the JWC as part of the preparation phase for a CAX and it is already proved to be a real value increasing the effectiveness and facilitating the accomplishment of a CAX overall objectives.

**Aim**:

The course is designed to provide the students with a basic knowledge package about NATO exercises and training. It is focused to develop the operator skills and required for an effective conduct of a CAX. The final aim is to create a pool of national CAX specialists aware of the CAX support tools used in the Response Cells during NATO CAX's.

**Security Classification**:

None requested Security Clearance. M&S COE request to enroll the course to fill up the RFV, request for visit and the PAF, personnel administration folder. The overall classification of the course is Non sensible Information Releasable to the Public – NATO Unclass. It is open only to NATO Military & Civilian members.

**Target Audience**:

- **Rank Level** : The course is eligible to enrol by Officers (OF), Other Ranks (OR), Civilians of all fields due to take part in Steadfast and Trident Series and other NATO CAX
- **Language Proficiency**: Language skills: English : 3,3,3,3. Attendees should be familiar with Windows package.

**Training Strategy**:

- The Course objective is to disseminate information, in 8 days; the course has been designed to ensure that personnel attending NATO exercises are able to support the various phases, including Execution, in the best possible way. The Bi-SC Directive 75-7, Education and Individual Training, is the base for the course. For information, the course covers the following parts:

- Main Events List and Main Incidents List & JEMM
- NATO M&S COE
- NATO CAX Specialist Certification Course
- CAX Exercise Process
- NATO Exercise Centers
- CAX Process – BiSC Dir 75-3
- Exercise & Excon Structure
- Exercise Scenario
- JEMM Hands- on
- DB & C2 Process
- BiSim & VBS3 Overview
- JCATS Introduction
- JTLS Land-Air-Maritime-SOF Basic Orders
- CAX Mini-EX1,2
- Future for CAX

**Number of Students per year 2018**:

24 (all certified) Students from the following Nations:

- 10 (ITA);
- 3 (CZE);
- 3 (POL);
- 2 (USA;
- 2 (DEU);
- 2 (SVK);
- 1 (GRC);
- 1 (NOR).

**Depth of Knowledge**:
An estimate of the depth of knowledge to be achieved through the course is:
Level 200 – Foundation Skills and Competences Concept Knowledge Level

### 5.2 NATO Exercise Support, M&S Integration Specialist Course

JCATS is the constructive simulation system used for training below the joint operational level in NATO. In order to maintain solid supportability of this kind of training and exercises, M&S specialists with both NATO exercise know-how and JCATS user skills are needed. The Course was designed and developed by the JFTC, M&S COE and is directed to trained simulation practitioners from national training centers, having basic skills in JCATS, which are sufficient to execute common commands and procedures in the simulation with limited guidance.

**Aim**:

The course is designed to provide the students with a knowledge package focused on NATO exercises and training principles. It will help to develop the skill set required to effectively conduct M&S support focused below the joint operational level in NATO. The final objective is to enhance knowledge of national M&S specialists by creating awareness of the NATO-specific simulation issues. These include knowledge on the broad technical environment of JCATS-based simulation use cases in NATO and related M&S support tools and procedures used in NATO training events. In particular, concept and practicalities of federation is a primary focus, as applicable in many multi-national and multi-level training exercises.

**Security Classification**:

None requested Security Clearance. M&S COE request to enroll the course to fill up the RFV, request for visit and the PAF, personnel administration folder. The overall classification of the course is Non sensible Information Releasable to the Public – NATO Unclass. It is open to NATO Military & Civilian members .

**Target Audience**:

- **Rank Level** : The course is eligible to enrol by Officers (OF), Other Ranks (OR), Civilians of all fields .
- **Language Proficiency**: Language skills: English : 3,3,3,3.

  Attendees should be familiar with Windows package.

**Training Strategy**:

The Course objective is to disseminate information, in 8 days, this course is designed to enhance JCATS skills and NATO exercise expertise and by that develop personnel ready to augment M&S support to training and exercises in NATO, as well as for national use (e.g. exercises in preparation for NATO operations. For information, the course covers the following parts:

- Introduction to CAX in NATO
- M&S related tasks to NATO CAX process
- MEL/MIL design & execution process
- JCATS Land
- JCATS AIR, Maritime, SOF
- Interoperability in CAX
- Federation of models – Hands on (Mini-ex)
- Course completion test – Way ahead

**Number of Students per year 2018**:

**17** (all certified) Students from the following Nations:

- 10 (ITA);
- 2 (NOR);
- 2 (USA);
- 2 (EST);
- 1 (DAN).

**Depth of Knowledge**:

An estimate of the depth of knowledge to be achieved through the course is: Level 200 – Foundation Skills and Competences Concept Knowledge Level.

### 5.3 NATO Modelling & Simulation Basic Course

The Course have been created in order to satisfy the exigency of military and civilian personnel working in training and research oriented facilities to get the fundamental knowledge of military M&S solution and applications.

**Aim**:

Provides to the attendees a basic education in the field of Modelling & Simulation (M&S), through the knowledge of theory, processes, techniques, procedures and technologies oriented to M&S NATO & PfP military purposes .

**Security Classification**:

None requested Security Clearance. M&S COE request to enroll the course to fill up the RFV, request for visit and the PAF, personnel administration folder. The overall classification of the course is Non sensible Information Releasable to the Public – NATO Unclass. The NATO M&S Basic Course is also open to Partners as follows:

- Euro-Atlantic Partnership Council (EAPC)
- NATO‘s Mediterranean Dialogue (MD)
- Istanbul Cooperation Initiative (ICI)
- Partners across the globe (Afghanistan, Australia, Iraq, Japan, Pakistan, Republic of Korea, New Zealand, Mongolia)
- International organization (UN, EU, OSCE)

**Target Audience**:

The course is eligible to enroll by Officers (OF), Other Ranks(OR), Civilians of all fields. Language skills: English : 3,3,3,3. Attendees should be familiar with Windows package. Given the topics touched during the

course, an intermediate knowledge of Statistic, Probability and Mathematics is recommended for a better comprehension.

**Training Strategy**:

The Course objective was to disseminate basic information, in 4 days, on the use of Modelling and Simulation in a military context. For information, the course covers the following parts:

- Introduction to M&S, M&S Organization in NATO context
- M&S applications in military: classification based on M&S Master Plan
- Statistics, Probability and Randomness for M&S
- Modelling & Simulation Life Cycle
- Model Development & Simulation – Hands On
- M&S Supporting CD&E
- M&S in Support of Collective Training – Computer Assisted Exercises
- Interoperability - Distributed Simulation (Simlab)
- M&S Supporting CD&E use case: Simulated Interactive Robotics Initiative & M&S Way Ahead
- M&S Supporting Experimentation Use Case: CWIX & M&S Focus Area, M&S LL in Concept Development and Experimentation.

**Number of Students per year 2018**: Will be known in November 2018, we eastimate similar attendance as in 2017 –

**27** (all certified) Students from the following Nations:

- 16 (ITA);
- 3 (DEU);
- 2 (SVK);
- 2 (LIT);
- 1 (DAN);
- 1 (USA);
- 1 (CAN);
- 1 (NOR).

**Depth of Knowledge**:

An estimate of the depth of knowledge to be achieved through the course is: Level 200 – Foundation Skills and Competences Concept Knowledge Level.

### 5.4 ADL 211 – NATO MODELLING & SIMULATION CADET Course V.3.0

The course was developed to teach the attendees in order to deliver them the basic knowledge and the foundation skills that should enable the audience to deal and understand M&S issues in the military applications.

**Aim**:

The course on the fundamentals of Modelling & Simulation was developed by NATO M&S COE. It covers the origin of military M&S, basic terminology used in the M&S domain and classification of M&S applications according to the NATO Modelling and Simulation Master Plan.

**Security Classification**:

UNCLASSIFIED

**Target Audience**:

Rank Level: The course is eligible for Officers (OF), Other Ranks (OR), Civilians of all fields.

**Language Proficiency**:

English listening: 2; reading: 2.

**Training Strategy**:

Placed on NATO platform www.jadl.act.nato.int, in the COE's section, realized with a dedicated software for the creation of e-Learning courses, it serves as the introduction into the M&S as a potential military discipline. It is an instrument to indoctrinate those who want to approach the world of Modelling & Simulation and for those who will be directly involved at the frequency of all COE's residential course and above all sewed for the M&S Basic residential courses. User, after requested the membership, on the above mentioned NATO platform and obtained the access by ACT site managers, is evaluated by COE' course administrator that will or not execute it. Then he/she will need a minimum of 80% to pass a final test and 100% ( all modules in green) in the learning progress to complete the course and get a certificate, signed by COE's Director.

**Number of Students per year 2018**:

**65** Students after the introduction of the renamed course (v.3.0), from different Nations (the system (ilias) does not permit to know their Nationality):

**18** (COMPLETED);

**45** (IN PROGRESS);

**2** (NOT ATTEMPTED).

**Depth of Knowledge**:

Intermediate Level – 200

# 6. CWIX 2018 MODELLING & SIMULATION FOCUS AREA REPORT

Maj. C. Tondo

NATO Modelling and Simulation Centre of Excellence, Rome (ITA)

Ing. Marco Picollo

Leonardo company, Land & Naval Defence Electronics

## 6.1 Methodology

The M&S Focus Area was organized in a large complex federation using a Distributed Simulation Agreements Document. These provided guidelines and direction to establish configuration settlements among the simulation applications required to support simulation interoperability and to stimulate real Command and Control Systems for CWIX 18.

## 6.2 Challenges

- Many interactions with other FAs were simultaneously established, the main challenge was to coordinate the different testing activities of the participating capabilities. The adoption of a Distributed Simulation Agreement (DSA) reduced but did not prevent completely uncontrolled situations and loops, but did help to solve quickly these situations whenever they occurred.
- Supporting Joint Vignettes and coordinating all the different contributions was very interesting and challenging for the Focus Area, lessons learned from the past years were of paramount importance to mitigate the risk of jeopardizing M&S relevant activities.
- In summary the simulation systems participating in the M&S Focus Area generally accomplished their objectives. The M&S Focus Area proved once again how M&S is a fully interoperable enabler, being able to provide distributed services that can support the Commanders' and their Staffs' training during exercises (i.e. Joint Vignette), as well as their speed of decision making before and during operations, experimentation and development of new concepts of operations, doctrine and procedures. New systems and nations participated for the first time, bringing in new energies, ideas and opportunities. Visitor and VIP day brought guests showing a strong interest in attending next

CWIX, this will help to enlarge the M&S area of interest and participation in CWIX.

### 6.3 Summary

- CAN MSAAS #144. Canada participated for the third time with a modified MSAAS 1.0 simulation infrastructure and implemented a remote station located in Canada. This allowed a new expanded and complex set of test cases to be run and to introduce multi-national, multi-domain network infrastructure to the simulation interoperability challenge. The introduction of long-haul distributed simulation within the NATO environment to the Canadian Joint Warfare Centre was a significant improvement from previous CWIX events and will be planned for future CWIX participation within the M&S functional area. The goal and objectives were achieved which will provide a solid foundation to build upon for expansion of its capability.
- The DEU-DFTOPaaS #7 (DFTOP as a Service) capability managed to conclude nearly all its test cases successfully. The big challenge was to design and implement a distributed service architecture, the Data Farming Services (DFS), first as the basic prerequisite to integrate the former desktop application DFTOP into this architecture as a service. The future goal will be that each DFS service can be accessed from all over the network according to the Federated Mission Networking (FMN) concept. DFS will be dynamic, scalable and interchangeable as a Docker-Architecture. At first, DFS was operated on a stationary server. On the way to FMN, DFS services were successfully hosted on the DEU Mission Network (i.e. DEU Demonstrator) as the DEU national FMN instantiation. The DFS are compatible and interoperable. DFS was accessible via the DFS-Portal on the GMN Portal. The next step was to conclude the DFS concept and to distribute all the DFS via CFBL Network between JFTC in Bydgoszcz, POL and Taufkirchen/Munich, DEU. After the successful implementation, the DFS service based interface to exchange data with TOPFAS was successfully tested. In order to test the bidirectional data exchange, TOPFAS was extended by a DFS Interface to connect to DFS and load documents from the Analysis Result Repository and integrate those into TOPFAS documents. The transfer worked without any issues. In external test cases, it was possible to analyse and visualize the data of the FIN Live-Simulation Data recorded at exercises in DFTOPaaS. The Test was successful and it was agreed to working together in future. Additionally, it was possibnle to convert different virtual-machines (Hyper-V and VMWare) and deployed these into the NATO Modelling

& Simulation Centre of Excellence (MS COE) infrastructure and vice-versa.

- Interoperability Challenges The main interoperability work was the integration of DFS into GMN and the collaboration with the NCIA to implement the TOPFAS integration. Both of which were tested successfully. Limited success was achieved in the test cases regarding the cross security domain communication of all services. The main issue here was that not only the data but all communication between the services had to be labelled. This included control messages and special messages regarding CORS (Common Origin Resource Sharing), a browser safety feature to protect against cross site scripting. Improvements from CWIX 2017 was a successful DFTOP stand-alone demonstration as a client application. The improvement at CWIX 2018 are, the development of DFTOP as a part of the Data Farming Services and a technical further development to DFTOPaaS as a scalable, distributable, interchangeable IT-Service using Docker Technology. A second step forward was the DFTOP - TOPFAS integration along with the tested interoperability with TOPFAS as a NATO planning tool in use. The interface was implemented and validated. And finally, last but not least, DFS is compatible with GMN and thus has proven to support FMN. This was seen as an important prerequisite for the DFS implementation in FMN Spiral 4 M&S.
- LIVEBIGDATACONSINTEG #130 capability has been tested as planned with partners. Two tests were innovated and done outside of the originally planned tests. Successful test results gave answers to some previously unanswered questions. KASI data could be use in different ways with other systems. DFTOP will work very well also as a tool of analyzing training data. In future constructive simulators, like the MARCUS system, it is only possible to use old live simulation data in several ways. MARCUS was very flexible system to demonstrate this idea. This will give possibilities, for instance, to validate models, reducing the need of operators, making a more realistic training simulation, testing new methods of fighting, testing different systems and supporting training. Data construction and preparing data was key aspect in tests. Most of that work was done before the CWIX 2018 exercise.
- FIN was participating for their first time in the M&S Focus Area and it is possible that this participation will pursue onto CWIX 2019 with similar ideas but a more complex system. Man-in-the-loop Virtual Asset (MVA)#135 is in experimental state and CWIX 2018 has been the second opportunity to test the system into a complex heterogeneous

environment made by a variety of different software interacting with different standards. The software upgrade, with the possibility to create a scenario, not only one single entity, has been widely operable. The introduction of the geographical filter turned out to be a necessity in high resources demanding scenarios, to ensure stability and reliability. The new features of HCI, guarantee a more comfortable and faster operator actions.

- JFTC participated in CWIX 2018 with the following three capabilities: NATO-JFTC-JCATS #149, NATO-JFTC-JLOD #151 and NATO-JFTC-Pitch RTI #260. NATO-JFTC-VBS3 #152 was withdrawn before execution. During execution development stage versions, JCATS 14.0 and JLOD 6.0, were used in parallel with the fielded versions JCATS 13.1 and JLOD 5.0. The development stage versions were stable and provided new features that were useful and highly appreciated. Pitch RTI version 5.3.2.1 was used to generate simulation federations. JFTC participated in 68 test cases related to the FA Objectives, either as a provider, a consumer or a mediator with the following capabilities: JLOD, VBS3, ITA_SGA, ITA LVC GTW, ITA_MVA, ITA_DITB, CAN_MSaaS, US_MUSE, US_ISIM, US_IEWTPT, SVN_3D Viewer, SVN_C2 Sim Gateway and IVCT from M&S FA as well as NIRIS, NCOP, TUR ADVENT-SIM, POL JASMINE, ICC, and ITA SIACCON. Additionally, the JFTC capabilities participating in the Joint Vignette provided almost all simulated tracks for the stimulation of C2 systems for all five Joint Vignettes. The majority of the test cases were assessed and the outcome was a “success”. One test case (00351) was withdrawn because by mistake the Verification Process included steps that were not in line with the CONSUMERS capabilities.
- Another test case was created based on the appropriate Verification Process. A few test cases faced interoperability issues because there was some required functionalities that were not provided by JCATS.
- JFTC contributed to the coordination of the tests by providing a Federation Coordinator (sharing the responsibility with an M&S COE expert). They also contributed the internal M&S Lessons Learned process by providing a LL coordinator who was responsible to collect, organize and analyse the M&S related observations inserted into the CWIX ODCR.
- NATO JWC-VBS3 Collector #274. JWC provided VBS3 and Collector capability to fulfill requirements for JISR FMV distribution and to run it in a federated environment. Compared to the previous year, the configuration that JWC set up allowed creating new vignettes. In

addition, streamed constantly from the UAV assets to the network and easily federated VBS3 with the other DIS federates. VBS3 was connected to NIRIS, and was able to share the UAV track to other C2 systems to support joint vignettes. Due to VBS3 limitation, air tracks did not have Mode 3/C neither any Call signs, however they were identified by speed, altitude, location, and bearing.

- FMV was streamed via Collector as a STANAG compliant stream to several consumers as well as to VLC media player and portrayed in the Air FA room. VBS3 was federated with MUSE, JCATS, USA IAMD, and a German fighter simulator. Interaction between those did not bring any problems except some minor issues. IAMD aircraft was able to make a strike on VBS3 entity successfully and VBS3 air defense assets were able to fire on and shut down IAMD flying assets . As always, the main interoperability issue is the DIS enumeration. Due to fact that VBS3 does have limited number of 3D models there was a need to portray some remote objects of different entities. NATO JWC-VBS3 Collector system was very stable and all test cases were finished with the success status.
- NATO JWC-JTLS #273. To fulfill the Training Audience requirements, Joint Warfare Centre uses Joint Theatre Level Simulation (JTLS®) to simulate forces on the ground and to stimulate training Audience C2 systems during execution phase of the NATO exercises. JTLS is an interactive simulation that models multi-sided air, ground, and naval civil-military operations with logistical, Special Operation Force (SOF), and intelligence support. The 2018 testing will include JTLS 5.0 and major NATO C2 systems – ICC, MCCIS and LC2IS. Interoperability with a new version of ICC3.2 has been verified, in scope of creating ICC database, parsing ACO and ATO into JTLS, then executing JTLS air orders based on that and finally producing proper MissRep into ICC. MCCIS testing includes ship tracks feeds from JTLS, various settings, variants and other options have been verified. The LC2IS testing consists of land force ORBAT reports produced from JTLS into LC2IS, in form of AdatP3 formatted messages as well as direct LC2IS feed. Direct interface between JTLS and LC2IS, producing .sif files and it is a new functionality that was not present in earlier versions of JTLS. SIF is a native LC2IS file format storing all force related information. This interface is still in the development phase and required further improvements. In addition, JTLS produced KML files with ORBAT information. They were then uploaded successfully into Sitaware SIM-C2 Gateway provided by SVN. KML is well recognized format of data used e.g. by Google

Earth. Also a new version of JTLS 5.1 has been tested, considering fact is it not official release yet.

- NATO-MSCOE-LVC GTW #357 tested 2 main components: LVC Gateway and C2Bridge (NFFI and MIP DEM Block 3.1). As LVC Gateway, NATO-MSCOE-LVC GTW Capability confirmed to be able to make federations using different protocols, and to make them exchange data in real time. It used:
  - PITCH 5.3.2.1 RTI federation (RPR FOM version 2.0 D17) with protocol HLA 1516e;
  - MAK (3.3.2, 4.2, 4.4.2 ) RTI federation (RPR FOM v. 2.0 D17, revision 2 and 6) with protocol HLA 1516;
  - DIS (v. 6 and 7) data. NATO-MSCOE-LVC GTW also performed a fine tuning between all the different federates; it proved to be an essential tool to:
    - investigate and debug errors
    - normalize all the federates to common .fed file and .rid file
    - apply a real time mapping, modifying attributes between two federates
    - help each federate to map unknown objects.
- Therefore, the system administrator has, at a glance, the picture of the overall traffic and is able to manage it. In case of issues, he has the possibility to:
  - examine in detail every single object and its attributes,
  - adjust some attributes in real time of a entering or exiting federation,
  - filter a suspicious object in order to prevent to be distributed to all the federations,
  - split a federation into two, isolating malfunctioning federates,
  - feed a federation with new objects created by MoSiM GTW with the purpose to test interactions, aggregations or the overall functioning of the federation.
- NATO-MSCOE-LVC GTW upgraded its functionalities also during the tests following the needs of other participants. It gave evidence to be a real "capability" and not only an application. NATO-MSCOE-LVC GTW-C2 Bridge component created a node MIP 3.1 acting as a Reporting Unit named LVCGW_SIMREPUNIT. It received and

represented all the data of the simulation. Using the protocol MIP DEM, it sent data to DEU_JHQ_MESBW and ITA_BDE node. In conclusion, NATO-MSCOE-LVC GTW proved to be an essential tool to manage complex exercises using simulated or real/simulated data.

- NATO-MSCOE-LVC GTW (component BridgeC2) was the provider of simulation data generated by NATO-JFTC-JCATS forward the Joint Vignette. NATO-MSCOE-LVC GTW created a node MIP 3.1 acting as a Reporting Unit named LVCGW_SIMREPUNIT. It sent updated Situation Awareness to Land Component Command (LCC) DEU_JHQ_MESBW by protocol MIP DEM. NATO-MSCOE-LVC GTW applied several filters to represent the scenario agreed with LCC. This function simplifies the management of report units (reducing cost and limiting the numbers of LOCON operators) during CAX exercises.
- Interoperability Challenges Tests within the MAK HLA federation were quite challenging when performed on systems installed in different subnets (MAK graphic Assistant cannot be used). In this case, a RID file had to be created and configured in order to overcome MAK graphic Assistant limitation. Improvements from previous CWIXs NATO-MSCOE-LVC GTW, by its component C2Bridge, operated as provider of simulation data to forward C2 systems during the Joint Vignette.
- NATO-MSCOE-SGA #147 capability achieved good results this year in its two main objectives: participating to the M&S FA federation based on DIS and HLA standards, providing M&S services, and testing FMN Spiral 4 specifications about virtualization technologies in the Future Core Services FA. The new capability version was successfully tested and in particular, its new HLA-evolved interface has proven to be able to connect and interact with different RunTime Infrastructures (RTIs) and modular Federation Object Modules (FOMs). Tests with the new version of the IVCT tool were also accomplished. Simulation data regarding IFF and electromagnetic emissions have not been tested deeply and so it remains as a recommendation for next year.
- NATO-MSCOE-GATEWAYSIMREAL #344 capability successfully accomplished its objective about interconnecting M&S capabilities with real command & control systems. It translated Joint Vignettes running in the M&S FA to NIRIS Link 16 JREAP-C track store for Operational Command use. It has been offered as an M&S service to all partners in need of stimulating C2 systems and vice versa. The main interfaces tested were Link16, OTH-Gold and NFFI and GATEWAYSIMREAL filtering system was also successfully tested. It also consumed GEOMETOC FA WMS services.

- NVG interface in CWIX this year for the first time, was not tested since NCOP was not supporting version 1.5 during the exercise. Increasing use of filtering functions, NVG interface and a new VMF interface could be a recommendation for the next year to test.
- NATO-MSCOE-IVCT #342 capability was tested in CWIX for the second time. This year the system was upgraded to the newest release 1.0 coming out from NATO STO MSG-134 outputs and now maintained by the new-formed NATO STO MSG-163. The tests were performed using Executable Test Cases (ETCs) developed for CWIX experimentation purposes and mainly covered basic HLA verifications and objects publications. IVCT used only Pitch RTI as the infrastructure for the federation. Recommendations for next year could be to test with different RTI vendors and with an increased number of ETCs.
- SVN-3D VIEWER #325. SVN participated for the first time with SVN-3D VIEWER. 3D Viewer is a geospatial application offering a 3D visualization, manipulation and analysis of spatial data. It reads HLA data from a federate system and shows entities in 3D environment. The M&S FA performed 8 test cases, 4 were successful, 4 with limited success. The goal and objectives were achieved. Results will provide a solid foundation to build upon for expansion of its capability.
- SVN-C2 SIM GATEWAY #154. SVN participated for the first time with SVN-C2 SIM GATEWAY. The IFAD SIM Gateway enables live, virtual and constructive (LVC) systems to actively participate in distributed simulation exercises. The SIM Gateway is used to link live systems and simulators into integrated test beds, training environments and distributed simulation exercises. IFAD SIM Gateway uses the Distributed Interactive Simulation (DIS) and High Level Architecture (HLA) standards for run-time scenario data exchange. The M&S FA performed 7 test cases, 5 were successful, 2 with limited success. The goal and objectives were achieved. Results will provide a solid foundation to build upon for expansion of its capability.
- ADVENT SIM#367, the TUR System, is currently in developmental stage, although it participated in CWIX-2018 with a complete range of functionalities based on HLA federation protocol. The system was tested by federating both MAK and PITCH RTI Systems. Test cases were completed successfully. Additionally, DIS connection successfully handled by the means of gateways - LVC-GW and SGA capabilities provided by the NATO M&S COE - and VR-Exchange, an

internal tool of ADVENT SIM. The system is fully compatible with HLA1516 and HLA1516e standards.

- ADVENT SIM system was tested publishing and consuming air, surface, subsurface entities, publishing and receiving emitter, publishing active sonar, detecting fire and detonation interactions, performing an accurate evaluation of over 500 entities interactions. The main goal was achieved connecting the capability directly to NATO PITCH RTI System without any protocol translation provided by the already mentioned gateway. In this case, all of the services worked well. This will allow us to join several more capabilities next CWIX.
- A few problems were experienced with the Multicast transmission because the VLAN was different from the M&S Focus Area VLAN. M&S participants also encountered some minor problems with some of the partner capabilities, especially ones that use DIS based systems.
- C2 - simulation interoperation (C2SIM #368) is a cooperative project between NATO MSG-145 and the Simulation Interoperability Standards Organization (SISO). They aim at a capability for coalitions to get standards-based interoperability of their C2 and simulation systems. The vision is that C2SIM will enable a coalition by simply connecting together their systems of training, course of action analysis, and mission rehearsal. MSG-145 has eight national teams cooperating to develop and test the C2SIM technology, while SISO has a Product Development Group developing a standard that MSG-145 expects to become the basis of a STANAG. The overall C2SIM process has arrived at a point where it should be exposed to some operational military training and subjected to rigorous testing. Both of those goals are supported by bringing C2SIM to CWIX 2018. Five nations are supporting the testing process, which involves the NORCCIS C2IS from NOR, the KORA simulation from DEU, the JSAF simulation operated by the GBR, and the VR-Forces commercial military simulation. The required server and editor, are provided as open source software by the George Mason University C4I and Cyber Centre (USA), which is also testing a server enhancement that emulates a cyber-active environment for military training. A multi-stage testing process, from simple connection to a complex counter-insurgency scenario, has been completed with success.
- USA-JMSC-IEWTPT #310. Intelligence and Electronic Warfare Tactical Proficiency Trainer (IEWTPT) participated as a first use case in a multinational environment, with 14 documented test cases. Although IEWTPT facilitates multiple proficiencies at all echelons of the Intelligence Warfighting Function (IWF), testing objectives were

limited to validating the capability of select NATO allies to consume simulated JSTARS Ground Movement Target Indicators (GMTI). GMTI was successfully passed to NOR DOT Matrix (a GMTI Client and the equivalent to the US MOVINT Client). An additional opportunity test with SWE was successful in that GMTI was passed to the SWE CSD (Coalition Shared Data) server. SWE did not have a GMIT Client (MOVINT equivalent) available to subscribe to the feed. Of note, IEWTPT's normal protocol is to publish to an IP and allow a MOVINT client (or similar) to subscribe and pull in GMTI. However, in both NOR and SWE tests, a UDP feed was pushed to the consumers due to capability limitations of partner nations. This is significant because it validates a different way to use IEWTPT in a Multinational environment. IWETPT also received entities from JLOD during federation testing.

- US-JMSC-JCATS #303. JMSC's Joint Conflict and Tactical Simulation (JCATS), a constructive simulation, conducted interoperability testing with MARCUS, its HUN counterpart, (Capability #315) for the second consecutive CWIX. The ultimate goal of this testing remains building the option to use a JCATS- MARCUS Federation for a simulation supported exercise. Conducted over four documented test cases, each test case tested multiple smaller events. Over all, the testing achieved limited success and no significant improvements from last year. It was found that artillery fire, direct fire, movement, terrain navigation and cross federation simulation troop movement worked as expected. Counter fire radar did not work due to the design of MARCUS IDF shot PDUs. Another limitation is MARCUS obstacles such as minefields do not affect JCATS entities. However, the biggest limitation this year was the load testing. MARCUS was only able to handle just over 60,000 entities before we started to see latency issues. This is directly the result of their hardware. The HUN only brought one computer to serve as the client and the server, and this computer was significantly limited in its processing memory capacity.
- US-JMSC-MUSE #305. Multiple Unified Simulation Environment (MUSE), a simulated UAS ISR platform, was used to support the development of other nation’s capabilities and test US GCCS-A/J ability to ingest FMV and telemetry. MUSE participated in 18 documented test cases, most of which were supporting the Joint Vignettes for other nations or capabilities to test. Rather than using SIRIS to provide the FMV distribution, the federation manager and Air Focus Area lead decided to use NIRIS as the FMV inject point. Multiple customers were using the NIRIS as a published and

subscribed capability. MUSE was successful to see all entities published in JCATS v14.0 as well as VBS3. MUSE also participated in testing with USA-GCCSJ to ingest MPEG-2 video with telemetry and H.264 video with telemetry. In both tests, GCCS-J was able to receive FMV but unable to receive telemetry.

### 6.4 Recommendations

- Distributed Simulation Agreement (DSA) proved its usefulness so it is recommended to fill it in with even more details during the conferences and before the execution and, above all, enforce its adoption to all Focus Area participants.
- In order to fully support Joint Vignettes, which is run almost all over the CWIX, it is better to duplicate if possible the involved M&S capabilities. If ignored, the risk could jeopardize M&S testing.
- It is recommended to increase the interaction with FMN-related FAs for testing the services offered by the M&S FA against FMN Spirals specifications.
- Undertake more comprehensive testing to exchange Simulation data and electromagnetic emissions with IFF at CWIX 2019.
- At CWIX 2019, test the interoperability between NVG interface and a new VMF interface.
- At CWIX 2019 test the IVCT capability with different RTI vendors and with an increased number of ETCs.
- In these years, M&S as a Service (MSaaS) architectures has been tested from a service point of view, verifying the consumption of their services while instead, interoperability among M&S as a Service capabilities in CWIX, has never been tested. Exploring and experimenting this aspect, especially in coordination with NATO STO MSG 164, could be a recommendation for the next year.
- Data Farming and Big Data were a very important first experimentation for us. They could be a key point for further activities in the future, in coordination with NATO STO groups, especially in testing the capabilities providing Big Data to be consumed by Data-Farming systems and producing useful outputs for predictions and decision-making support. In addition, an interesting point to be further assessed as a possible contribution of such capabilities to Joint Vignettes and Operational Command FA.

# 7. CWIX 2018 – CYBER FOCUS AREA SUPPORT – OCEAN INFRASTRUCTURE[11]

Davide BRUZZI, Christian FAILLACE, Marco PICOLLO

Leonardo company, Land & Naval Defence Electronics

LTC Marco BIAGINI, Massimo PIZZI

NATO Modelling and Simulation Centre of Excellence

## 7.1 Executive Summary

This document aims to detail the technical activities provided by Leonardo to ACT in support of the Cyber Range federation, interoperability and resilience activities, which were executed in the Cyber Focus Area (FA) during the NATO Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise 2018 (CWIX18) execution.

Introducing the activity, is provided an overview about the infrastructure that the NATO Modelling and Simulation (M&S) Centre of Excellence (CoE) designed applying the Leonardo Open Cloud Environment ApplicatioN (OCEAN) solution.

More in detail a description of the system is provided in order to better describe its architecture from a network point of view.

In the core part of this report the phase of testing is presented, with an explanation of the general purposes and the specific use cases played through different VPN layers: the first one was about the cyber range federation, and the second one was about the distributed Malware Information Sharing Platform deployment and availability.

The success of this experimentation activity represents a step forward towards the demonstration of the potentiality of application of a distributed synthetic system based on services over cloud.

[11] Extracted from the original report of Leonardo company, version 1.0 of 02 July 2018

## 7.2 Introduction

The CWIX is the largest annual NATO event gathering different stakeholders providing a federated multi-functional environment in which scientists eXplore emerging interoperability standards and solutions through collaborative innovation activities, Engineers eXperiment with new interoperability solutions and assess suitability for near term implementation, Testers eXamine technical interoperability among fielded and soon be fielded capabilities and generate scorecards, and Operational users eXercise interoperability capabilities using a relevant scenario.

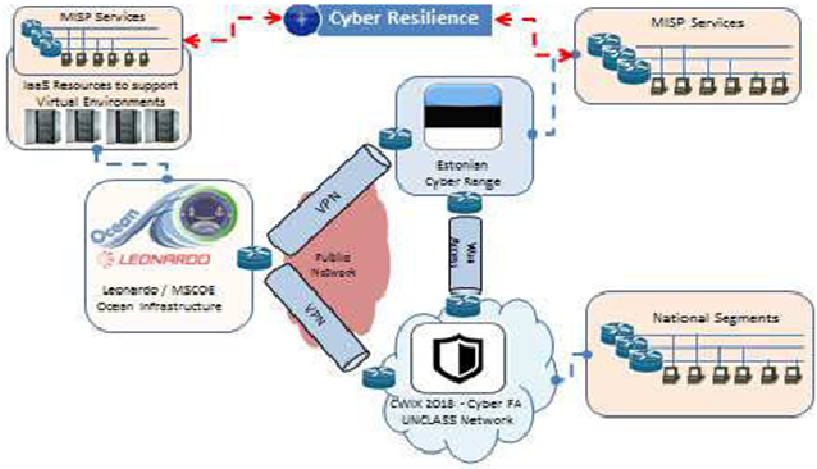



**Figure 7-1**

Part of CWIX18 Cyber Focus Area activities aimed to investigate interoperability and service resiliency between cyber ranges. In order to perform these tests, a capability that performed as a partner for the Estonian Cyber Range was identified in the Leonardo OCEAN Infrastructure, provided for CWIX activities through NATO M&S CoE. The OCEAN infrastructure was designed and developed in collaboration with the M&S CoE to offer an embryonic framework made of a combination of hardware, software and services to automate the deployment of M&S tools and applications in a cloud environment to support the development of a Governmental Cloud- Based M&S as a Service Infrastructure (MSaaS).

For this experiment OCEAN Infrastructure was re-configured and set up as an additional environment, hosting resources typically allocated in a Cyber Range and it was connected to the Estonian Cyber Range (CR.EST), providing a Governmental Cloud capability under the Infrastructure as a Service paradigm, mainly dedicated to host Virtual Machines (VMs).

More specifically, Cyber Range interoperability was investigated and experimented with OCEAN Infrastructure being integrated in cyber services resiliency testing (Cyber Resilience), by providing redundancy for Malware Information Sharing Platform (MISP) services. Such testing was conducted as CWIX18 / Cyber FA Objective *"To explore cyberspace resilience regarding mission critical services federation, using the EST Cyber Range and M&S COE Cyber Range"*.

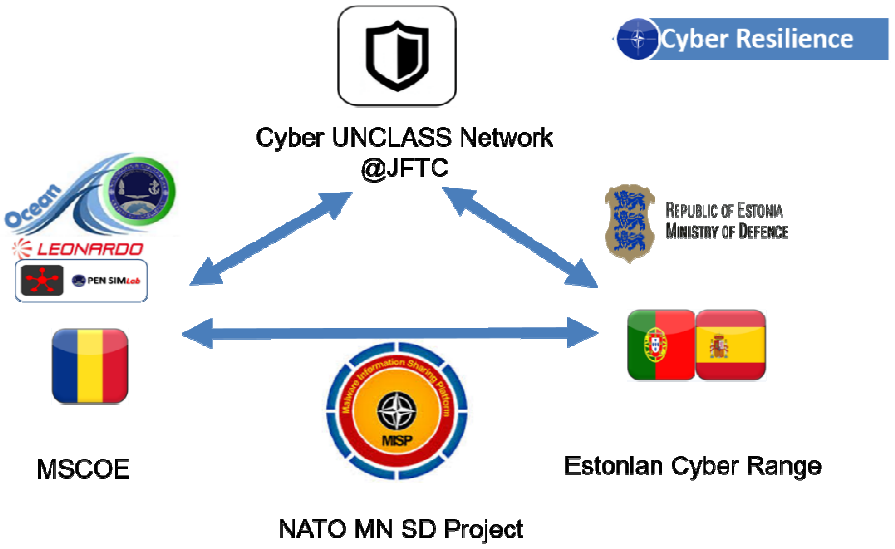



**Figure 7-2**

## 7.3 Experiment Architecture

The architecture of cloud services and network connectivity that was created to fulfil the cyber resiliency testing requirements, involved three main sites that are the Joint Force Training Centre (JFTC) in Bydgoszcz (POL), CR.EST in Tallinn (EST), and OCEAN Infrastructure allocated in the OPEN SIMLAB BattleLab at NATO M&S CoE in Rome (ITA).

Each site was connected with the other two, in order to allow proper services access and synchronization, so the geographically distributed topology of the testing architecture has involved creation of dedicated and reliable Virtual Private Networks (VPNs) between each site.

A VPN was established by a Multiprotocol Label Switching (MPLS) Layer 2 tunnel providing services of Internet Service Provider (ISP). Then, VPN1

and VPN2 were established by having each site firewall interacting though public network.

General Internet Protocol (IP) addressing plans and routing structures for Cyber FA and Cyber Ranges internal networks, as well as the internal IP for VPN tunnel connections, were established in advance as part of the Cyber FA planning.

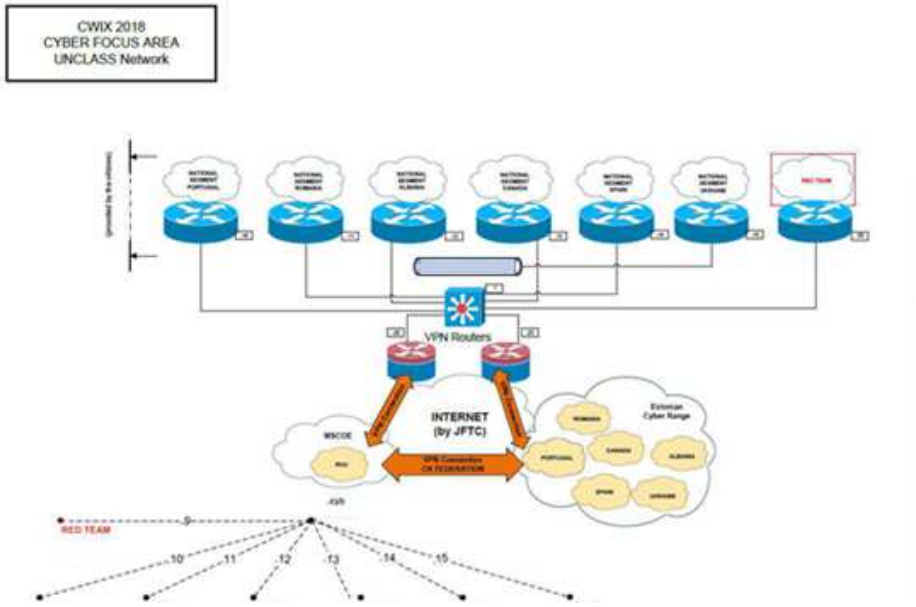



**Figure 7-3**

The other main aspect involved in establishing this cyber resiliency testbed is the VM deployment and availability, in which CR.EST and OCEAN had to import and deploy user provided VMs inside their virtualized infrastructure, to be available for remote site such as JFTC.

## 7.4 Experimentation Activities

Two Test Cases were performed during the experimentation activities in the Cyber FA using OCEAN. Tests focussed on networking and systems federation, identifiable as follows:

- Test case for the Federation of Cyber Ranges by using Layer3 VPN form different provider. This layer3 connection was mainly used for MISP synchronization between EST and OCEAN M&S COE Cyber Ranges. MISP in EST Cyber Range was operated by Portugal (PRT); MISP in the M&S COE Cyber Range OPEN SIMLAB is operated by Romania (ROU).

- Test case for the ROU-Cyber-Unclass should access, configure, and use MISP Virtual Machine located in M&S COE Cyber Infrastructure.

### 7.4.1 Test Case: Cyber Range Federation

Federation of cyber ranges has been implemented by ensuring that VM related to cyber services from both sites could communicate and share data through a dedicated link. Such data exchange was ensured at an application level within the MISP-to-MISP REST interfaces, relying on a Layer 3 IP address planning and network reachability.

A dedicated VPN was established for MISP Virtual Machines located in both Cyber ranges to be able to synchronize between CR.EST and OCEAN.

VPN was created between Firewall devices directly connecting to public network with public address, and directly connected to Cyber Range internal networks dedicated to Cyber Resiliency testing, in order to provide little or no internal routing for MISP VM access.

The established configuration allowed creation of a stable, Internet Control Message Protocol (ICMP), tested, encrypted VPN tunnel, which showed little to no loss of packet.

Network monitoring allowed to identify that a bug, encountered in the VPN negotiation and re-negotiation process, which happened every 3600 seconds, with a result of roughly 10 ICMP packet loss over 3600 (<1%).

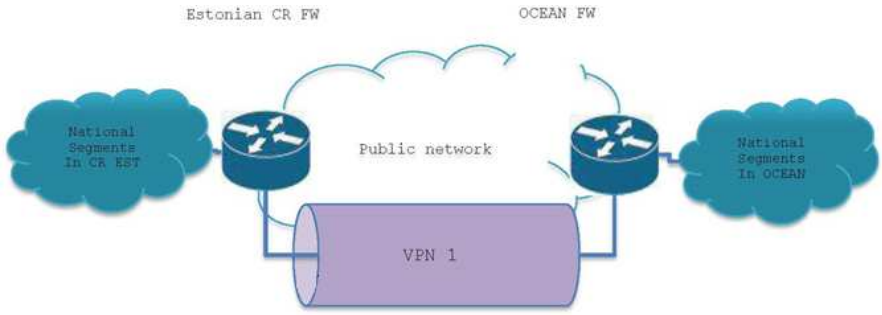



**Figure 7-4**

Log analysis showed that such bug was caused by use of Internet Key Exchange (IKE) v1 in the negotiation process, which supports only re-authentication. IKE v2, which was not usable to due to lack of compatibility between the two different vendor's equipment used for the VPN implementation, would have allowed for new keys exchange to happen without any interruption of the existing IKE and IPsec Security Associations.

### 7.4.2 Test Case: Distributed MISP Deployment and Availability

Malware Information Sharing Platform (MISP) has been chosen a pilot service to allow for resiliency testing over a distributed network. MISP Services rely on a single, independent VM that can federate to each other in order to share alerts and indicator of compromise (IOCs) received from Security Information and Event Management (SIEMs). VM to be sued for Cyber-Resiliency testing have been prepared in advance by involved nations from CWIX18 Cyber FA.

Practically, before the exercise ROU MCIS Agency provided a preconfigured VM that was uploaded to M&S COE and imported in OCEAN infrastructure.

As the uploaded VM did not have a network configuration that was compliant to the IP addresses assigned OCEAN network segments, nor did it allow for any remote management other than the MISP service browser based https interface.

MISP service interface is not suitable for any configuration of operating system parameters, both because it allows little configuration for this and is better suited for Cyber Security operations, so login and password for privileged access at operating system level were provided by ROU MCIS Agency.

Accessed through OCEAN Infrastructure consoles interface, the MISP VM was configured accordingly to IP address and routes plans, and a secure shell server (Open SSH) was installed to allow for any further remote configuration. Network reachability for this VM was then tested on local network up to OCEAN main firewall.

As Romanian MISP VM was deployed, in order to achieve network reachability, a second dedicated VPN was established from OCEAN towards JFTC. For this, a vendor router was dispatched form M&S COE towards JFTC, with a pre-established configuration for remote access and tested template for vendor-to-vendor equipment VPN implementation.

Defining a set of VPN negotiation and encryption parameters, was carried out as a pre-configuration task before shipping the router to JFTC, so the main difficulty was in adapting those parameters to Network Address Translator (NAT) environment and public IP in JFTC.

Logs and real-time monitoring showed heavy IP and port scanning on the router translated public address, which was dealt with by cooperating with JFTC network staff, and restricting access of JFTC public IP address to OCEAN public IP address, as a JFTC firewall policy.

As VPN template was still not functioning, Maximum Transfer Unit (MTU) size adjustment was investigated, as well as tracerouting internal and external networks routing issues or reachability, and finally OCEAN firewall policies accuracy in order to prevent unwanted packet filtering.

Analysis showed that NAT in JFTC was causing IKE negotiation in phase 1 to fail on one vendor equipment side, the template used for that vendor's firewall to establish connection was modified from site-to-site VPN, which didn't preview that remote site may be behind NAT, to a client-to-site VPN that allows NAT-traversal capabilities.

Such template allowed the VPN to be established through the NAT, and internal tunnel reachability between VPN tunnel interfaces, but not network-to-network reachability from Cyber FA planned IP ranges, limiting such reachability to JFTC router tunnel interface.

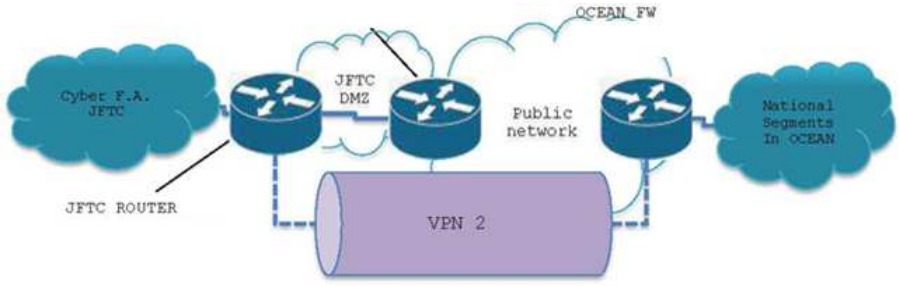



**Figure 7-5**

As applicative communications for MISP services were planned to be client-to-server from JFTC to OCEAN, solution was implemented as having the JFTC router performing overload NAT / masquerading towards OCEAN networks, thus allowing for full reachability form JFTC clients to OCEAN cloud-hosted MISP service

## 7.5 Conclusions

The use of M&S CoE's OCEAN Infrastructure within the CR.EST, to achieve an interoperable Cyber Range federation, based on different VPN's Layers, was accomplished. It allowed the further successful cyber-services resiliency testing activity for the CWIX2018 Cyber FA, and in particular:

- The Cyber Range and MSaaS Infrastructures federation was investigated and established, as OCEAN has been connected to CR.EST and to JFTC Cyber FA Unclassified network, by VPNs over public network. MISP services were successfully integrated inside OCEAN cloud infrastructure, so availability and effective use of these services from JFTC was achieved, as well as creating a MISP

Federation for data synchronization between services in OCEAN and CR.EST.

- The Infrastructures federation allowed cyber services resilience to be successfully achieved, as MISP service was available in JFTC and proved resilient to single VMs unavailability, while MISP in OCEAN or MISP in CR.EST were alternatively shut down following test case procedures. To this extent, OCEAN MSaaS infrastructure has been successfully tested as a service provider for integration and resiliency testing purposes through remote access. Import and deploy of customer provided systems and VMs as flexible networking and virtualization structure ensured reliable use of assets from inside the OCEAN infrastructure towards JFTC.

Considering time consumption and problem solving needed for each task, it should be noted that infrastructures and services federations were established quite seamlessly, as both were relying on proven and tested interfaces between systems, such as OCEAN Infrastructure with VMware virtualization and local networking paradigms, and MISP. Most problems in these areas were solved with good cooperation between services providers and consumers.

On the other hand, network interconnection requested time for setup, dealing with different implementations of network tunnelling and encryption. Future implementations of similar Cyber Range Federations should therefore plan for network setup as much soon as possible, while tacking great care to hardware vendor interoperability (best if all sites use network devices form the same vendor), VPN and network parameters agreements, and laboratory network configuration tests as thorough as possible.

### 7.6 Way Ahead

The outcomes of this successful experimentation activity opens to the MSaaS new opportunities. From an M&S perspective the deployment of OCEAN to federate Cyber Ranges is the first building block to develop and implement an interoperable M&S-based environment (Cyber Synthetic Environment) to further provide M&S services (Cyber Synthetic Services). OCEAN is proposed as one of the first Governmental Cloud Solution for modelling and Simulation services, and it has proven that has the potential to further extend and improve Cyber Range Federation Capabilities also with the support of Modelling and Simulation tools. This area is still under development and investigation by the M&S CoE that is developing and promoting, across the Alliance, the NATO Cyber Synthetic Environment Concept.

# Part III

# WHITE PAPERS

# 8. REQUIREMENTS AND EXAMPLE FOR A C2SIM EXTENSION TO UNMANNED AUTONOMOUS SYSTEMS (UAXS)[12]

Lt.Col. Marco BIAGINI, Maj. Fabio CORONA

NATO Modelling and Simulation Centre of Excellence

Fabrizio INNOCENTI, Stefano MARCOVALDI

Vitrociset company

## 8.1 Executive Summary

The "Command and Control Systems to Simulation Systems Interoperation (C2SIM) is a family of standards for expressing and exchanging Command and Control (C2) information between C2 systems, simulation systems, and robotic and autonomous systems (RAS) in a coalition context" [1].

C2SIM replaces the Coalition Battle Management Language (CBML) [2], for describing task and report messages in operational or simulation systems, and the Mission Scenario Definition Language (MSDL) [3]. The latter for initializing the operational environment (terrain, units, weather conditions, COAs, simulation checkpoints, etc.) in a wide variety of simulation and connected systems. C2SIM has been being developed starting from a core Logical Data Model (LDM), which provides at a logical level a set of data elements common to most C2 and simulation systems, combined with a standard way to adding to that core a collection of additional elements specific to a particular domain.

The NATO M&S CoE, has been performing Concept Development and Experimentation activities to support NATO Allied Command for Transformation (ACT) since 2016 and in particular supporting the Countering UAxS Project [4] and now the Autonomy Program. In particular, the Centre is investigating the employment of Unmanned Autonomous multi-domain Systems (UAxS) in the modern battlefield, with specific focus on their deployment in high-populated mega-cities in 2035. This future scenario [5] poses several issues regarding, among all, the

[12] Excerpt from M&S COE "C2SIM Extension to Unmanned Autonomous Systems (UAXS) – Process for Requirements and Implementation" white paper released to NATO STO MSG panel.

interoperability with traditional troops, UAxS' tactics, techniques and procedures, UAxS levels of autonomy and their behaviours, and finally Command and Control (C2) in mission command. Experimentation is necessary to address these issues and to proof the concept to find possible solutions, includeing adopting Concept Development Assessment Game (CDAG) [6] and Disruptive Technology Assessment Game (DATG) [7] techniques. Modelling and Simulation (M&S) tools and architecture are essential to speed up this process in a cost effective way, and C2SIM is a possible candidate to be a standard interoperable language between C2 systems and UAxS.

The NATO Framework Architecture (NAF) [8] adequately adapted, was used to collect and describe the requirements for extending the C2SIM core LDM to the UAxS domain, in the framework of the "Operationalization of Standardized C2-Simulation Interoperability (C2SIM) activity [9], in collaboration with industry [10]. The UAxS extension development process was addressed by the Distributed Simulation Engineering and Execution Process (DSEEP) [11] approach, applying the SISO guidance for the conceptual scenario development [12]. The requirements and the simulation environment architecture were formalized, through operational views applying the NAF methodology.

With the "Research on Robotics Concept and Capability Development (R2CD2)" project, the M&S CoE, supported by the Italian Ministry of Defence and in collaboration with the industry and academia developed an operational scenario to be used within a federation of simulators and C2 emulated Systems implementing the C2SIM extension for UAxS. In the first stage of the project CBML eXtensible Markup Language (XML) schemas were extended, since at that time C2SIM core schemas were not yet available.

The document illustrates the NATO M&S COE's proposal to include in the C2SIM UAxS extension ontology, still under development, XML schemas for UAaS' Air Tasking Orders and reports. These C2SIM schemas were built comparing and improving the CBML schemas developed for the R2CD2 project with the C2SIM core schemas defined to support the MSG-145 experimentation activities during the Coalition Warrior eXploration, eXperimentation, eXamination, eXercise (CWIX 2018)..

## 8.2 Introduction

The draft of the C2SIM standard by the Simulation Interoperability Standard Organization (SISO) Product Development Group (PDG) states that the "Command and Control Systems to Simulation Systems Interoperation (C2SIM) is a family of standards for expressing and

exchanging Command and Control (C2) information between C2 systems, simulation systems, and robotic and autonomous systems (RAS) in a coalition context." [1]. This means that the new C2SIM Interoperability Language, C2SIM for short, replaces the Coalition Battle Management Language (CBML) [2], for tasks and reports, and the Mission Scenario Definition Language (MSDL) [3], for scenario initialization. Therefore, the C2SIM is developed for describing task and report messages in operational or simulation systems, and for initializing the operational environment (terrain, units, weather conditions, COAs, simulation checkpoints, etc.) in a wide variety of simulation and connected systems. In order to cover several application areas, C2SIM is developed starting from a core Logical Data Model (LDM), which provides at logical level a set of data elements common to most C2 and simulation systems. Then, one of the goal of the new standard is defining a way to add to that core a collection of additional elements specific to a particular domain.

The NATO M&S COE supports the NATO Allied Command for Transformation (ACT) with its own Concept Development and Experimentation activity on the particular domain of the employment of the Unmanned Autonomous Systems (UAxS) in the modern battlefield. Specifically, particular focus is on UAxS deployment in high-populated mega-cities in the mid and long term. This future scenario poses several issues regarding, among all, the interaction with traditional troops, UAxS' tactics, techniques and procedures, UAxSs levels of autonomy and their behaviour, and finally Command and Control (C2) in mission command. In this context, C2SIM is a good candidate to be a standard interoperable language between C2 systems and UAxS. Rigorous experimentation is necessary to address these issues and proof future solutions envisioned in a Concept Development process. Modelling and Simulation (M&S) tools and architecture are essential to speed up this process in a cost effective way and support concept experimentation. From this standpoint, NATO M&S COE is working to provide M&S methodology, techniques and tools suitable to support proof of concept and experimentation activities within the Concept Development Assessment Game (CDAG) and Disruptive Technology Assessment Game (DATG). In particular CDAG is "a qualitative analytical method for assessing concepts or conceptual documents. It can be described as an open table-tom analytical war game" [6]. On the other hand, DTAG is a methodology for "some common understanding regarding technologies which might have a significant or even disruptive impact on future threats, operational needs, and long-term planning" and to "bring together the technological and the military perspective" in an interactive process [7].

NATO M&S COE already conceptualized a first M&S platform to address concepts experimentation needs regarding UAxS operational deployment

back in 2016 [4]. Afterwards, the CoE dealt with a standard methodology for the development of an operational scenario [5]. For that aim, the SISO Guideline on Scenario Development for Simulation Environments (GSD) [12] was applied to an air-reconnaissance scenario involving UAxS in an urban environment. This methodology was demonstrated to be suitable to support the requirements development for future UAxS capabilities, in term of platforms, doctrine, procedures and kind of countermeasures, as well as M&S tools for proof-of-concepts. The same methodology, adequately adapted, was used to develop a UAxS scenario in collaboration with the Fraunhofer FKIE Institute (GER) [10] in the framework of the "Operationalization of Standardized C2-Simulation Interoperability (C2SIM)" tasking activity (MSG-145) [9] of the M&S Group panel of the NATO Science and Technology Organization (STO). The UAxS were commanded and controlled through C2SIM and this approach was effective to highlight the UAxS peculiarities and needs in that scenario, in order to express the requirements for extending the C2SIM core LDM to the UAxS domain.

All the results from past study activities were applied to the "Research on Robotics Concept and Capability Development (R2CD2)" project in order to generate a scenario involving UAxS operating in a mega-city of the future (2035), in two operational domains (air and land) and interoperating with real C2 systems. In details, the process followed was inspired by the SISO GSD Distributed Simulation Engineering and Execution Process (DSEEP) [11] approach, and the NATO Framework Architecture (NAF) views were used for the formalization of the conceptual scenario, requirements and simulation environment architecture. Once, all the requirements for models, behaviors, C2SIM extension to autonomous systems, and simulation environment were expressed, and a first demonstrator was built with Industry and Academia support. It was an M&S-based platform built on open standard architecture, made of selected constructive simulators, a C2 system and a gateway. At that time, CBML eXtensible Markup Language (XML) schemas were extended according to the requirements for the generation of the messages needed in the executable scenario, since C2SIM core schemas were not yet available.

In the first part, this document illustrates the general process followed in the R2CD2 project to generate requirements for extending the C2SIM LDM to autonomous systems, other than for models, behaviors, and simulation environment architecture. Moreover, the simulation environment is described in details.

The second part of the document goes into details of the data elements that extend the CBML XML schemas to autonomous systems and that NATO M&S COE proposes to include in the C2SIM UAxS extension ontology

under development. These XML schemas are for both the Air Tasking Order to the UAV swarm of the R2CD2 scenario and the reports generated by the same UAV swarm. All the messages generated during the execution of the R2CD2 scenario are based on these schemas. All the detailed descriptions of each data element are skipped in this excerpt.

Finally, an example of a C2SIM extension to autonomous system developed by the M&S CoE was produced. The C2SIM core schemas recently defined for the experimentation during the last edition of Coalition Warrior eXploration, eXperimentation, eXamination, eXercise (CWIX 2018) were considered and compared to the CBML schemas of the R2CD2 project with the helpful collaboration of the George Mason University partners. All the data elements which could find a correspondence in the already defined core schemas were highlighted and mapped. Therefore, all the missing information needed for the R2CD2 scenario were included in the C2SIM schemas and isolated to build a first example of extension of the C2SIM core schemas to autonomous systems. The new C2SIM UAxS extension schema is not included in this excerpt.

## PART I

In this part of the document the process followed to generate requirements for extending the C2SIM Logical Data Model (LDM) to autonomous systems is illustrated, as it was applied to the scenario development of the "Research on Robotics Concept and Capability Development (R2CD2)" project. This process follows the SISO GSD [12] and uses the NATO Framework Architecture (NAF) views to formalize the conceptual scenario, requirements and simulation environment architecture.

### 8.3 Scenario Development Process

According to the SISO GSD a military scenario development process begins with the definition of the simulation objectives, usually involving military users and specifying the application domain, one instance of the application space. Therefore, the Operational Scenario is produced according to the operational, functional, technical, organizational and economical requirements. It can be also in written form, expressing what, where, when to be represented. Then, a first structured description of all scenarios to be executed in the simulation environment is produced, defining what is called "problem space". At this point, the Conceptual Scenario can be defined as an implementation-independent representation of a single scenario which satisfies all the previously defined requirements. Finally the Simulation Environment to execute the scenario can be designed and developed. Figure 8-1 illustrates the single steps of the process, making a comparison between DSEEP process and the SISO GSD steps with relative deliverables.

In the following the single SISO GDS steps are developed for the R2CD2 project scenario.

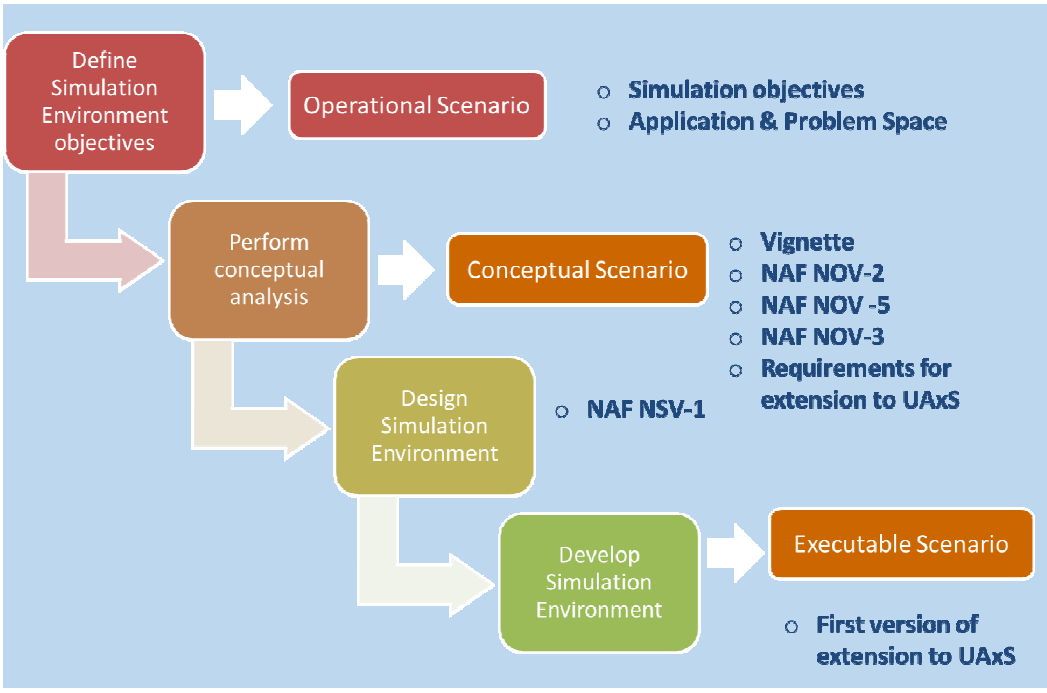



**Figure 8-1: DSEEP and SISO GSD steps comparison .**

### 8.3.1 Scenario Objectives

The main high level simulation objectives for the R2CD2 project scenario are:

- interaction between simulated UAxS and real C2 systems;
- study of UAxS employment in a megacity of the future;
- consideration of two operational domains for UAxS (Air and Land);
- use of C2SIM Interoperability Language for messages (Orders & Reports) and study of requirements for C2SIM extension to UAxS, either live or simulated.

The scenario should help to find those peculiarities of the UAxS, such as the level of interaction with humans and decision making capacity, which should be include in the extension of the C2Sim LDM core, not already covered by the Maneuver Warfare extension. The employment of the UAxS should be possibly justified by a dangerous or lethal environment for humans. The terrain should be an example of future urban environment.

Figure 8-2 shows what can be considered the NAF OV1, a general high-level description of the scenario under development.


**Figure 8-2: NAF OV1 of R2CD2 scenario**

### 8.3.2 Application Domain

In this refining process of the scenario, starting from the scenario objectives a particular application domain (an instance of application space) of the scenario can be defined as follows:

1. Simulation Application Mode: Concept Development & Experimentation;
2. Capability: Unmanned Autonomous Systems Analysis and Interoperability with C2 systems;
3. Military level: Tactical to Operational;
4. Kind of mission: urban counter-IED;
5. Staff involved: Subject Matter Experts (SMEs) on Robotics, Interoperability Languages and Data Models and on Modelling and Simulation (M&S).

### 8.3.3 Operational Scenario

A threat, which consists of an unknown vehicle loaded with explosive, moves around in a mega city of the future. Already alerted, police patrol detects and recognizes it, so they communicate some data of the vehicle for identification. In order to contrast the threat robotic autonomous systems in small units are employed as friendly forces. In particular, in the air domain, a swarm of Unmanned Autonomous aerial Systems (UAaS) for a reconnaissance mission to find the threat and report about its position, and, in the land domain, a team of Unmanned Autonomous ground Systems (UAgS) for neutralization of the threat. Each team has its own command

post which assigns the mission to be performed autonomously by the robots according to a level of autonomy appropriate for the mission. The autonomous systems report back to their command posts according to the level of autonomy assigned. The UAaSs have to perform the reconnaissance mission, report about the position of the target, so the UAgS team is activate for a C-IED mission to neutralize the target.

### 8.3.4 Problem Space

Defining the "problem space" means to set all the common features of all possible scenarios which respect all requirements fixed in the previous development steps, so simulation objectives and the operational scenario have to be considered. The following elements make the problem space:

1. Terrain

Since the terrain should be a mega city of the future for CD&E study on autonomous systems in urban environment, a piece of the ARCHARIA model developed for the ACT Urbanization Project (UP) [13] by the NATO M&S COE is used. The model is already an example of mega-city of the future (2035), with a lot of envisioned problems (e.g., over-population, high density buildings, exposure to natural disasters, like a volcano or coastal tsunami) and reusing it is in-line with M&S principles for cost reduction and efficiency.

2. Order of Battle

The composition of enemy and friendly forces has to be set, in terms of number, level and type of units, with weapons and equipment as well. For the autonomous systems, the typology of UAxS has to be set, like the size category and application area, as well as their payloads, like weapons and/or sensors. In this case, the swarm of UAaSs is composed by Small (from 3 to 10 kg) platforms, equipped only with electro-optical sensor. The UAgSs have to be more robust and built for combat missions, especially in contaminated areas, where it could be dangerous to enter for the humans. They should be light armored and equipped with explosive for C-IED missions.

The enemy unit is a blue truck loaded with explosive.

3. Enemy Course of Action (ECOA)

In this scenario, the dangerous truck moves around the city, trying to not be detected, only to stop near a sensible spot and explode.

4. Level of Autonomy (LoA) of the UAxS

An important aspect to be set for an unmanned autonomous platform is their Level of Autonomy (LoA), since this parameter fixes the behavior of the UAxS and their interaction with their own command posts, meaning the rate of reports, if they need coordination and/or confirmation on the tasks to be performed, or if they can make their own decisions based on the feedbacks from the environments. In order to define the LoAs, NATO M&S COE reuses the results of the Autonomous Systems Countermeasures (C-UAxS) project [14] of the ACT. This concept development activity had the aim to envision the countermeasures against future enemy UAxS, analyzing their vulnerabilities. A conceptual experiment was conducted, called Disruptive Technology Assessment Game (DTAG), in order to develop future autonomous capabilities with a methodology based on role-playing [7]. As reported in the annex A to C-UAxS DTAG Experiment Results and Conclusions [15], seven levels of autonomy for UAxS have been defined, numbered from 0 to 6. These levels consider systems starting from "human controlled" to "fully autonomous", based on the degree of human interaction while performing their tasks, not depending only on the level of technology or the relation between the human operator and autonomous system. A LoA set the ability of the autonomous system to tackle the problems connected with the mission complexity or the difficulty of environment.

The levels of autonomy of UAxS defined during the ACT C-UAxS Project are described in Table 8-1. For example, a level 0 refers to a UAxS which are basically remote-controlled, while a level 3 system is a more properly autonomous system which coordinates with its HQ for determining its tasks, according to the feedbacks from the terrain, while level 5 is a fully autonomous system which will report only the results of the mission assigned. Level 6 is particular, because it refers to UAxS which are fully autonomous, but which can assign missions by itself depending on external conditions, thought for a non-traditional unit (i.e, insurgent or terrorist), dormant in the environment, which could activate itself. So, when the typology of UAxS is chosen for a scenario, it is important to set also its LoA.

**Table 8-1: The levels of Autonomy [15].**

| LoA | Operating functionality |
|---|---|
| **6** | Based on its knowledge of a broader environment, the system can initiate automatically a mission.<br><br>The system gathers, filters, and prioritizes data. The system integrates, interprets data and makes predictions. The system performs final ranking. No information is ever displayed to the human. The system executes automatically and does not allow any human interaction. |
| **5** | The system is tasked with a specific mission.<br><br>The system gathers, filters, and prioritizes data. The system integrates, interprets data and makes predictions. The system performs final ranking. The system executes automatically and does not allow any human interaction. Final results are displayed to the human. |
| **4** | The system is tasked with a specific mission.<br><br>The system gathers, filters, and prioritizes information displayed to the human. The system analyses to provide data that are integrated, interpreted and makes predictions into a result which is only displayed to the human if result fits programmed context. The system performs ranking tasks. All results including "why" decisions were made to the human. The system executes automatically, informs the human, and allows for override ability during execution. The human is shadow for contingencies. |
| **3** | The system is used for a specific mission.<br><br>The system gathers and displays all the information to the human, but it highlights the non-prioritized, relevant information for the user. The system analyses the information to provide data and makes predictions, though the human is responsible for interpretation of the data. Both the human and the system perform ranking tasks but the results from the system are considered prime. The system allows the human a pre-programmed context-dependent time to veto before execution. The human shadows for contingencies. |
| **2** | The system is used for a specific mission.<br><br>The system gathers and displays unfiltered, un-prioritized information for the human. The human still is the prime monitor for all information. The system is the prime source of analysis and predictions, with human shadow for contingencies. The human is responsible for interpretation of the data. Both the human and the system perform ranking tasks, the results from the human are considered prime. The system executes decision after human approval. The human shadows for contingencies. |
| **1** | The human gathers and monitors all data, with the system shadow for emergencies. The human performs analysis and predictions, with the system shadow for contingencies. The human interprets the data. The human performs all ranking tasks, but the system can be used as a tool for assistance. The human executes decision, with the system shadow for contingencies. |
| **0** | The human only gathers and monitors (defined as filtering, prioritizing and understanding) all data. The human analyses all data, predicts and interprets data. The system does not assist in or perform ranking tasks. The human must do it all. The human alone can execute decision. |

NOTE: the 0-2 levels always need the human operator as main resource for the decision on the tasks to be performed (e.g., UAV pilot).

### 8.3.5 Conceptual Scenario

#### 8.3.5.1 Initialization

The initialization of the conceptual scenario can be described by the following items.

1. Terrain

The terrain is a quarter of ARCHARIA, a model of a mega-city of the future (around 2015) as described above.

2. Order of Battle

Red Forces

An hostile truck, blue, with a known plate, loaded with explosive, moves around a quarter of a future mega-city.

Blue Forces

- a swarm of three small UAaSs, equipped with electro-optical sensor for reconnaissance missions;
- a team of five light armoured mechanized UAgSs, for counter-IED missions.

3. LoA

The Level of Autonomy of UAaSs is equal to 3 with reference to Table 8-1: they are tasked with a mission and they can elaborate intermediate tasks, but always ask the humans for confirmation. They always report back or display to humans the feedbacks of their sensors.

The Level of Autonomy of UAgSs is equal to 5 with reference to Table 8-1: they are tasked with a mission, they perform it according to tasks which they elaborate autonomously and don't ask to humans for confirmation. They report to humans at the end of the mission.

4. ECOA

The hostile truck moves around the quarter of the city, trying to not be detected, only to stop near a sensible spot in order to explode.

#### 8.3.5.2 Vignette

In the following the flow of the actions and information exchanged during the execution of the scenario are described.

1. The UAaS command post (CP) receives an police alert about a truck bomb moving in an area of the city, thus it orders to the UAV swarm to search and follow the truck in the area (with an ATO) and send information on the target.
2. UAaS s search autonomously the target in linear formation, initially following waypoints inserted into the ATO, then searching the target in circular concentric trajectories according to implemented technical tactical procedures.
3. While moving, the UAaS s report about their own status in a General Status Report.
4. When the truck is found one UAaS follows it, sends back a video streaming of target and reports target's position and status (moving) in a Target Report.
5. The UAgS CP orders to counter-IED UAgS team to Be Prepared To take action (BPT order).
6. When the target stops the UAaS hovers over it and reports back target's position and status (holding) in Target Report.
7. The UAgS CP orders to counter-IED UAgS team to reach the location of the truck and to disposal the target.
8. The UAgS team performs autonomously the mission (clear area and disposal of the target) and reports back the outcome.
9. The UAgS team return to the base autonomously.
10. UAaS swarm receives the order to return to the base by its UAaS CP and it does it.

#### 8.3.5.3 NAF formalization

The NATO Architectural Framework (NAF) methodology can be used to describe in a more formal way the conceptual scenario described above. The NAF Operational Views (NOV) are very useful in order to identify:

- the entities (classes) to be created in the executable scenario, together with the interactions between them;
- tasks and activities;
- content of the messages.

In the NAF terminology, the items in the list above are the operational elements to describe an architecture from the operational standpoint. In particular the NAF view OV 2 (shown in Figure 8-3) is the "operational

node connectivity description" which defines all the logical operational nodes, the interconnections among them, activities performed and information exchange needs.

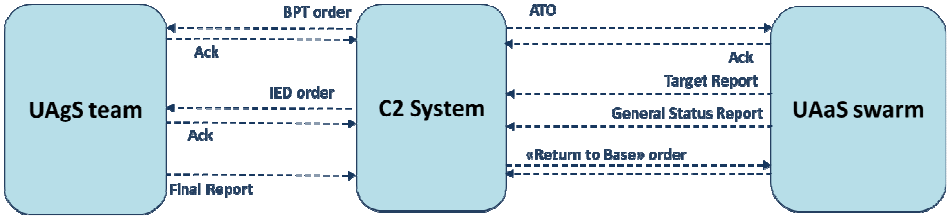



**Figure 8-3: NAF OV-2 of the R2CD2 project conceptual scenario**

The "operational activity model" or OV 5 (in Figure 8-4) represents the model of the activities performed by the operative nodes with the flow of the information, so the sequence of the activities and tasks is identified with the message exchange and the events and messages which trigger different actions.

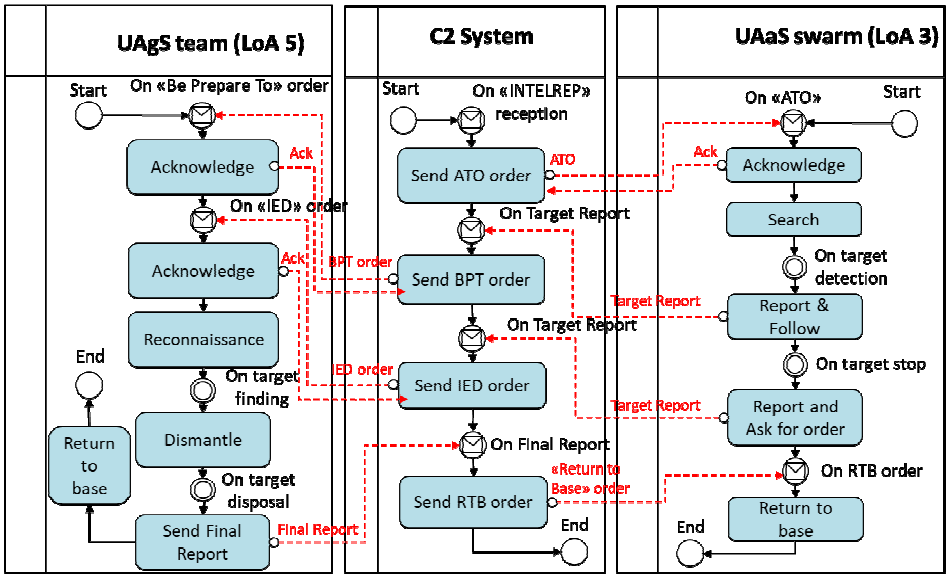



**Figure 8-4: NAF OV 5 of the R2CD2 project conceptual scenario**

Moreover, in support of the development of the messages in the executable scenario, the requirements for the information exchange among all the actors can be represented in Table 8-2, which is the "operational information requirements" NAF view or OV 3. Some references to the systems to be used for the executable scenario can be noted in the OV 3.

**Table 8-2: NAF OV 3 of the R2CD2 project conceptual scenario**

| Supported operational task | Message | Producer | Consumer | Information exchange Attributes Frequency Attributes | | |
|---|---|---|---|---|---|---|
| | | | | Format | Frequency/ temporization | Attributes |
| Command/ Send Search and Follow mission order | ATO | C2 (UAaS C2 GUI) | UAaS swarm (VR Forces) | XML file | once | |
| Report on target detection | Target Report | UAaS swarm (VR Forces) | C2 (MASA) | XML file in the "..\R2-CD2\UAaS\Outgoing\" | On event (target detection) | - TargetMovingStatus – Moving |
| Command/Send «Be Prepared to Mission» order | BPT order | C2 (MASA) | UGV team (Sword) | XML file in " ... bml_message\incoming\ " | On event (target detection) | UAgS systems in a state of "Ready for the mission" |
| Report on target stopping | Target Report | UAaS swarm (VR Forces) | C2 (MASA) | XML file in the "..\R2-CD2\UAaS\Outgoing\" | On event (target stopping) | - TargetMovingStatus: Holding<br>- Target position for IED order |
| Command/ Send IED order | IED order | C2 (MASA) | UGV team (Sword) | XML file in " ... bml_message\incoming\ " | On event (target stopping) | |
| Command/ Send return to base order | RTB order | C2 (UAaS C2 GUI) | UAV swarm (VR Forces) | XML file | On event (target disposal) | |

In order to pass from the conceptual scenario to the executable scenario, the design and the development of the simulation environment is necessary. In the following the logical architecture of the simulation environment of the R2CD2 project is illustrated, together with additional requirements for the messages to be exchanged.

## 8.4 R2CD2 Simulation Environment

In this section, the logical architecture of the simulation environment of the R2CD2 project is illustrated as developed by the NATO M&S COE in collaboration with the Industry.

The components of the logical architecture, depicted in Figure 8-5, are the following:

- SitaWare HQ by SYSTEMATIC as real C2 system;
- LVC Gateway by VITROCISET, as DIS/HLA -C2 Gateway;
- Sword by MASA as simulator for UAgSs with Artificial Intelligence (AI) add-on modules for autonomous behaviour and its BML connector;
- a TranslatorBML, which is a piece of software for generating BPT and IED orders for UAgSs from information read into reports from UAVs.
- VR-Forces by VT MÄK as simulator for UAVs with Artificial Intelligence (AI) add-on modules for flight behaviour and sensor feed management;
- CBML Parser for the UAaS simulator, as translator of CBML orders/reports to/from the UAaS simulator;

- UAaS ATO GUI for generation of the ATO (waypoints, parameters for flight formation, LoA, sensor, etc.)
- An HLA Run-Time Infrastructure (RTI) [16].

All the simulators are Commercial-of-the-Shelf (COTS) with AI add-ons for generating the UAxS behavior. All the messages are exchanged through a shared file system and translated by the developed ad-hoc interface for all simulators. The real C2 system is involved in the architecture through the DIS/HLA-C2 gateway to display the Common Operational Picture (COP). The LVC gateway translates DIS/HLA [17, 16] information to a NFFI [18] feed and shares entities and events between the two simulators through both DIS and HLA since the same HLA implementation cannot be used. Anyway, the HLA RTI is functional also to an enlargement of the architecture to include other simulators, like some specific ones for communication, cyber effects, weapon systems, platforms or environment agents, but the list could be endless. The overall idea is to have a modular and scalable simulation environment.

The future challenges will be:

- to use the real C2 system to generate order and read reports updating the COP, thanks to a C2SIM interface. At the moment, unfortunately, manufactures of such systems did not have sufficient commercial drive to do the necessary software development.
- to distribute the messages with a server/client architecture in order to have a real distributed architecture over the network. For this the use of the C2SIM Reference implementation Server developed by the George Mason University (GMU) is already planned, but the UAxS extension needs to be implemented in it.
- the UAxS extension should move from the CBML XML schemas to the C2SIM schemas, since a first implementation of the C2SIM core schemas were made available for the last edition of the CWIX exercise.

In the following all required information to be inserted in the exchanged messages, as defined in the conceptual scenario, are considered in order to establish the data elements necessary to extend the CBML XML schemas to generate messages for the UAxS scenario of the R2CD2 project.

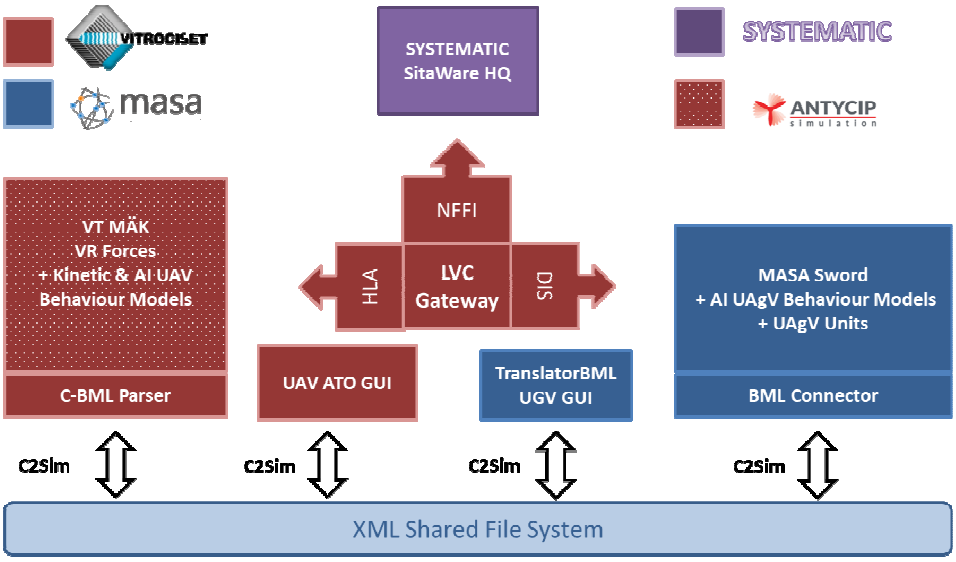



**Figure 8-5: Logical architecture of the R2CD2 project simulation environment**

## PART II

This part deals with the data elements that extend the CBML XML schemas to autonomous systems and that NATO M&S COE proposes to include in the C2SIM UAxS extension ontology under development. The messages considered are only those allow the interoperation in the air domain between UAaS command post and the UAaS swarm.

### 8.5 Extended XML schemas

In order to allow the exchange of the necessary information among autonomous systems implemented in the VT MÄK VR Forces simulator and other simulation systems and Command and Control Systems (C2) installed in the distributed synthetic environment under development at M&S CoE, two new XML schemas have been developed for C-BML messages, since it was not possible to extend the new C2SIM standard schemas which were not yet available at the time of this work.

The two new schemas are for:

- ATO (Air Task Order) messages to instruct one or more UAaS s to perform a mission
- Report thanks to which the UAaS s send back their status and position and the information about a possible threat detected

These two schemas are defined considering all the needed parameters for the execution of the UAaS s tasks and reusing, as components, all already defined C-BML structures if applicable.

In the next section these two schemas are described in detail.

### 8.6 XML Schemas Description

In this section the new developed message schemas are fully described.

For each message it will be given:

- The list of parameters contained in the message, together with a description
- The analysis about what in the message it is new and what it has been reused from C-BML standard

#### 8.6.1 Air Task Order (ATO) Message

The ATO message is used to instruct an UAV or a number of UAVs to perform certain tasks.

This message is altogether new at the root and has been built using components in part new and in part reused from C-BML.

The message format is described for its main parts in the following Table 8-3.

Substantially an ATO contains the following information:

- When the order have to be executed
- Who have to perform the task
- What has to be done
- With what the task has to be performed
- What target has to be looked for

**Table 8-3: ATO message format.**

| Types | Elements | Description | Values |
|---|---|---|---|
| ATO | | | |
| | AtoIssuedWhen | ATO date | |
| | AtoID | ATO Identification | |
| | AutonomyLevel | UAV autonomy level | Int 0-6 |

| | | | |
|---|---|---|---|
| | MinFuelLevel | Min acceptable fuel level | 0-100 % |
| | MinLinkQuality | Min acceptable communication link level | 0-100 % |
| | TaskList | Tasks ordered. Each task include the information below | |
| | TaskeeWhoRef | Who that is to carry the task | |
| | TaskActionCode | What is to be done | • Attack<br>• Move<br>• Loiter<br>• Hold<br>• Search<br>• Search and Follow<br>• Follow<br>• Home |
| | UAVFormation | Which type the formation the UAaS s are in | • Delta<br>• Line<br>• Column |
| | UAVBehaviour | Which type of behaviour the UAaS s are keeping | • Careless<br>• Stealth<br>• Aware |
| | TaskHow | Which type of sensor the UAaS s use to perform the task | • EO<br>• IR<br>• LIDAR<br>• SAR |
| | WhatTarget | What target the UAaS s are looking for | |
| | Route | The route to follow to perform the task | List of waypoints |

The definitions of the new defined ATO message fields are not included in this excerpt.

### 8.6.2 Report Message

The Report message is used so that an UAV or a number of UAVs can send back information about what they are doing.

This message is altogether new at the root and has been built using components in part new and in part reused from C-BML.

The message format is described for its main parts in the following Table 8-4.

Substantially a Report contains the following information:

- Who is sending the report
- When the report is sent
- What the report is about
- With what the report info have been collected
- What target has been found

**Table 8-4: Report message format**

| Types | Elements | Description |
|---|---|---|
| General status report | | |
| | TypeOfReport | The type of the report |
| | ReporterWho | Who is sending the report |
| | ReporterWhen | When the report is sent |
| | FuelLevel | Fuel level (0-100%) |
| | AutonomyLevel | Autopnomy level (0-6) |
| | LinkQuality | Communication Link level (0-100%) |
| | StatusWord | Status information |
| | Position | The current position of the UAV |
| | Attitude | The current attitude of the UAV |
| | ActionTaken | What the UAV is going to do |
| | ActionSuggested | What the UAV suggests to do |

| | | |
|---|---|---|
| | UAVFormation | The formation the UAVs are in |
| Target Report | | |
| | TypeOfReport | The type of the report |
| | ReporterWho | Who is sending the report |
| | ReporterWhen | When the report is sent |
| | SensorType | Which kind of sensor has been used to discover the target |
| | TargetStatus | Status of the target (Moving or Holding) |
| | TargetInfo | Information about the discovered target |
| | Position | The target position |
| | Type | Target Type (app6c code) |
| | Additional Info | Additional Info about the target |
| | Reliability | Reliability of the report (0-100%) |
| | Hostility | Hostility of the target (0-100%) |
| | ActionTaken | What the UAV is going to do |
| | ActionSuggested | What the UAV suggests to do |
| UnexpectedEventReport | | |
| | TypeOfReport | The type of the report |
| | ReporterWho | Who is sending the report |
| | ReporterWhen | When the report is sent |
| | Position | The target position |
| | Type | Event Type |
| | Additional Info | Additional Info about the target |
| | Reliability | Reliability of the report (0-100%) |
| | ActionTaken | What the UAV is going to do |
| | ActionSuggested | What the UAV suggests to do |
| CBRN report | | |

| | | |
|---|---|---|
| | TypeOfReport | The type of the report |
| | ReporterWho | Who is sending the report |
| | ReporterWhen | When the report is sent |
| | Position | The target position |
| | Agent | Radioactive material type |
| | Concentration | Agent concentration (0-100%) |
| | Reliability | Reliability of the report (0-100%) |
| | ActionTaken | What the UAV is going to do |
| | ActionSuggested | What the UAV suggests to do |

The definitions of the new defined Report message fields are not included in this excerpt.

## 8.7 Conclusions

In conclusion, this document illustrates the process to generate requirements for extending the C2SIM interoperability language to autonomous systems as applied in the context of the "Research on Robotics Concept and Capability Development (R2CD2)" project. This process follows the SISO guidelines for the development of a scenario and makes use of the NAF to formalize the conceptual scenario. In the second part, the new data elements proposed to support the information exchange in the scenario of UAxS are implemented in CBML XML schemas, since a C2SIM core XML schema was not available when this work was performed. Anyway, the same data elements can be included in an ontology which extends the C2SIM core LDM to autonomous system domain. The mechanism to generate C2SIM XML schemas for particular scenarios from C2SIM LDM core will be the subject of a guideline to be published by the SISO C2SIM PDG.

Within the scope of this document, the aim is to contribute to the work of the "Operationalization of Standardized C2-Simulation Interoperability (C2SIM)" tasking activity (MSG-145) of the STO NMSG providing inputs for

- extending the C2SIM core language ontology to the application domain of the autonomous systems;

- implementing this C2SIM UAxS extension LDM in the XML schemas which can be managed by the C2SIM Reference Implementation Server of George Mason University [19];
- supporting message schemas' generation for the experimentation of C2SIM UAxS extension in military simulated scenario involving UAxS.

### 8.8 Acknoledgments

The NATO M&S COE takes the opportunity to thank all the Industry for the fruitful collaboration in the "Research on Robotics Concept and Capability Development (R2CD2)" project. In particular, the VITROCISET company which is the main author of the first demo implementation of the CBML XML schemas extension to autonomous systems, subject of the second part of this document, and developer of the air domain part of the R2CD2 simulation environment. Moreover, NATO M&S COE thanks MASA group company, which developed all the land domain part of the same platform, making available also their system for the R2CD2 project. It cannot be forgotten that the results of this project would not be achieve without the availability of companies as Antycip and Systematic, which provided their products in the framework of technical agreements, according to the Open SimLab paradigm of the NATO M&S COE, a business model which foster collaboration and resource pooling among Government, Industry and Academia. Special thanks also to the GMU partners always very supportive during further experimentation of the extension.

### 8.9 References

[1] SISO C2SIM PDG/PSG, "Command and Control Systems - Simulation Systems Interoperation," 2016. [Online]. Available: https://www.sisostds.org/StandardsActivities/DevelopmentGroups/C2SIMPDGPSG-CommandandControlSystems.aspx. [Accessed Jun 2016].

[2] SISO-STD-011, "Standard for Coalition Battle Management Language Phase 1," 2014.

[3] SISO-STD-007, "Standard for Military Scenario Definition Language," 2008.

[4] M. Biagini and F. Corona, "Modelling & Simulation Architecture Supporting NATO Counter Unmanned Autonomous System Concept Development," in *MESAS 2016, LNCS 9991*, J. Hodicky, Ed., Rome, Italy, Springer, 2016, pp. 118-127.

[5] M. Biagini, F. Corona and J. Casar, "Operational Scenario Modelling Supporting Unmanned Autonomous System Concept Development," in *MESAS 2017, LNCS 10756*, J. Mazal, Ed., Rome, Italy, Springer, 2017, pp. 253-267.

[6] NATO STO SAS 086, "Maritime Situational Awareness: Concept Development Assessment Game (CDAG)," 2010. [Online]. Available: http://www.cso.nato.int/activities.aspx?pg=3&RestrictPanel=6&FMMod=0&OrderBy=0&OrderWay=2. [Accessed May 2016].

[7] NATO STO SAS 082, "Disruptive Technology Assessment Game - Evaluation and Validation," 2012. [Online]. Available: http://www.cso.nato.int/activities.aspx?pg=2&RestrictPanel=6&FMMod=0&OrderBy=0&OrderWay=2. [Accessed May 2016].

[8] NATO, "NATO Architectural Framework Documentation," 2018. [Online]. Available: http://nafdocs.org. [Accessed July 2018].

[9] NATO STO NMSG 145, "STO activities," 2016. [Online]. Available: http://www.cso.nato.int/activities.aspx?RestrictPanel=5. [Accessed May 2016].

[10] M. Biagini, F. Corona, M. Wolski and U. Shade, "Conceptual Scenario Supporting Extension of C2SIM to Autonomous Systems," in *22nd International Command and Control Research and Technology Symposium (ICCRTS)*, Los Angeles, CA (USA), 2017.

[11] SISO DSEEP PDG, "Recommended Practice for Distributed Simulation Engineering and Execution Process (DSEEP)," 2008. [Online]. Available: https://www.sisostds.org/stdsdev/tracking_final/doc_72/DSEEP_Draft2.pdf. [Accessed June 2017].

[12] SISO GSD PDG, "Guideline on Scenario Development for Simulation Environments," Simulation Interoperability Standards Organization, Orlando, 2016.

[13] NATO ACT, "NATO Urbanization Project," 2015. [Online]. Available: http://www.act.nato.int/urbanisation. [Accessed May 2016].

[14] NATO ACT CEI CAPDEV, "Autonomous Systems Countermeasures," 2016. [Online]. Available: http://innovationhub-act.org/AxSCountermeasures. [Accessed May 2016].

[15] NATO ACT CEI CAPDEV, "Disruptive Technology Assessment Game for Counter-Unmanned Autonomous Systems (C-UAxS) - Experimentation results and conclusions," North Atlantic Treaty Organization, Norfolk, 2016.

[16] IEEE SA STD 1516, "1516-2010 - IEEE Standard for Modeling and Simulation (M&S) High Level Architecture," IEEE Standard Association, 2010.

[17] IEEE SA STD 1278, "IEEE 1278.1-2012 - Standard for Distributed Interactive Simulation," IEEE, 2012.

[18] NSA STANAG 5527, "NATO Friendly Force Information (NFFI)," NATO Standardization Agency, 2008.

[19] George Mason University - C4I Center, "OpenBML," 2018. [Online]. Available: https://netlab.gmu.edu/trac/OpenBML.