NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-136)TP/830

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-136-Part-III**

Operational Concept Document (OCD) for the Allied Framework for M&S as a Service

(Document de définition opérationnelle (OCD) du cadre allié de M&S en tant que service)

Developed by NATO MSG-136.

Published May 2019

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-136)TP/830

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-136-Part-III**

Operational Concept Document (OCD) for the Allied Framework for M&S as a Service

(Document de définition opérationnelle (OCD)
du cadre allié de M&S en tant que service)

Developed by NATO MSG-136.

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published May 2019

ISBN 978-92-837-2156-7

Table of Contents

List of Figures

List of Tables

List of Acronyms

ACT	Allied Command Transformation
C2	Command and Control
CAX	Computer-Assisted Exercise
CGF	Computer Generated Forces
CPX	Command Post Exercise
DOTMLPFI	Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability
DSEEP	Distributed Simulation Engineering and Execution Process
EXCON	Exercise Control
IEEE	Institute of Electrical and Electronics Engineers
M&S	Modeling and Simulation
MSaaS	M&S as a Service
MSG	Modelling and Simulation Group
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NMSG	NATO Modelling and Simulation Group
NMSMP	NATO Modelling and Simulation Master Plan
OCD	Operational Concept Document
ORBAT	Order of Battle
SIMCON	Simulation Control
SISO	Simulation Interoperability Standards Organization
SLA	Service Level Agreement
SME	Subject Matter Expert
TAP	Technical Activity Proposal
UML	Unified Modelling Language
V&V	Verification and Validation

MSG-136 Membership List

CO-CHAIRS

Dr. Robert SIEGFRIED
aditerna GmbH
GERMANY
Email: robert.siegfried@aditerna.de

Mr. Tom VAN DEN BERG
TNO Defence, Security and Safety
NETHERLANDS
Email: tom.vandenberg@tno.nl

MEMBERS

LtCdr Tevfik ALTINALEV
Turkish Navy
TURKEY
Email: taltinalev@hotmail.com

Mr. Gultekin ARABACI
NATO JFTC
POLAND
Email: gultekin.arabaci@jftc.nato.int

Mr. Anthony ARNAULT
ONERA
FRANCE
Email: anthony.arnault@onera.fr

Col Thierry BELLOEIL
NATO ACT
UNITED STATES
Email: thierry.belloeil@act.nato.int

Dr. Michael BERTSCHIK
DEU Bundeswehr
GERMANY
Email: MichaelBertschik@bundeswehr.org

LtCol Dr. Marco BIAGINI
NATO M&S Centre of Excellence
ITALY
Email: mscoe.cde01@smd.difesa.it

Mr. Maxwell BRITTON
Department of Defence
AUSTRALIA
Email: maxwell.britton1@defence.gov.au

Dr. Solveig BRUVOLL
Norwegian Defence Research Establishment
NORWAY
Email: solveig.bruvoll@ffi.no

Dr. Pilar CAAMANO SOBRINO
CMRE
ITALY
Email: Pilar.Caamano@cmre.nato.int

Prof. Dr. Erdal CAYIRCI
Research Center for STEAM
TURKEY
Email: erdal@dataunitor.com

Mr. Turgay CELIK
MILSOFT Software Technologies
TURKEY
Email: tcelik@milsoft.com.tr

LtCol Roberto CENSORI
NATO M&S CoE
ITALY
Email: mscoe.ms08@smd.difesa.it

Maj Fabio CORONA
NATO M&S Centre of Excellence
ITALY
Email: mscoe.cde04@smd.difesa.it

Dr. Anthony CRAMP
Department of Defence
AUSTRALIA
Email: anthony.cramp@dst.defence.gov.au

Mr. Raphael CUISINIER
ONERA
FRANCE
Email: raphael.cuisinier@onera.fr

Mr. Efthimios (Mike) DOUKLIAS
Space and Naval Warfare Systems Center Pacific
UNITED STATES
Email: mike.d.douklias@navy.mil

Ing Christian FAILLACE
LEONARDO S.p.a.
ITALY
Email: christian.faillace@leonardocompany.com

Dr. Keith FORD
Thales
UNITED KINGDOM
Email: keith.ford@uk.thalesgroup.com

LtCol Stefano GIACOMOZZI
General Defence Staff
ITALY
Email: mscoe.ds02@smd.difesa.it

Mr. Sabas GONZALEZ GODOY
NATO ACT
UNITED STATES
Email: Sabas.Gonzalez@act.nato.int

Ms. Amy GROM
Joint Staff J7
UNITED STATES
Email: amy.m.grom.civ@mail.mil

Mr. Yannick GUILLEMER
French MoD
FRANCE
Email: yannick.guillemer@intradef.gouv.fr

Dr. Jo HANNAY
Norwegian Defence Research Establishment (FFI)
NORWAY
Email: jo.hannay@ffi.no

Mr. Andrew HOOPER
MOD
UNITED KINGDOM
Email: andy.hooper321@mod.uk

Mr. Willem (Wim) HUISKAMP
TNO Defence, Security and Safety
NETHERLANDS
Email: wim.huiskamp@tno.nl

Dr. Frank-T. JOHNSEN
Norwegian Defence Research Establishment (FFI)
NORWAY
Email: frank-trethan.johnsen@ffi.no

LtCol Jason JONES
NATO M&S CoE
ITALY
Email: mscoe.dr02@smd.difesa.it

Lt Angelo KAIJSER
Dutch Ministry of Defence
NETHERLANDS
Email: AJ.Kaijser@mindef.nl

Mr. Daniel KALLFASS
EADS Deutschland GmbH/CASSIDIAN
GERMANY
Email: daniel.kallfass@airbus.com

Col Robert KEWLEY
West Point
UNITED STATES
Email: Robert.Kewley@usma.edu

LtCol Gerard KONIJN
Dutch Ministry of Defence
NETHERLANDS
Email: gerard.konijn@gmail.com

Mr. Niels KRARUP-HANSEN
MoD DALO
DENMARK
Email: nkh@mil.dk

Mr. Vegard Berg KVERNELV
Norwegian Defence Research Establishment (FFI)
NORWAY
Email: vegard.kvernelv@ffi.no

Capt Peter LINDSKOG
Swedish Armed Forces
SWEDEN
Email: peter.j.lindskog@mil.se

Mr. Jonathan LLOYD
Defence Science and Technology Laboratory (Dstl)
UNITED KINGDOM
Email: jplloyd1@dstl.gov.uk

Mr. Jose-Maria LOPEZ RODRIGUEZ
Nextel Aerospace, Defence and Security (NADS)
SPAIN
Email: jmlopez@nads.es

Mr. Rene MADSEN
IFAD TS A/S
DENMARK
Email: Rene.Madsen@ifad.dk

Ms. Sylvie MARTEL
NCIA
NETHERLANDS
Email: Sylvie.Martel@ncia.nato.int

Mr. Gregg MARTIN
Joint Staff J7
UNITED STATES
Email: gregg.w.martin.civ@mail.mil

Mr. Jose Ramon MARTINEZ SALIO
Nextel Aerospace, Defence and Security (NADS)
SPAIN
Email: jrmartinez@nads.es

LtCdr Mehmet Gokhan METIN
Navy Research Centre
TURKEY
Email: m_gokhan_metin@yahoo.com

Mr. Aljosa MILJAVEC
MoD, Slovenian Armed Forces
SLOVENIA
Email: Aljosa.Miljavec@mors.si

Mr. Brian MILLER
U.S. Army
UNITED STATES
Email: brian.s.miller116.civ@mail.mil

Dr. Katherine MORSE
John Hopkins University/APL
UNITED STATES
Email: Katherine.Morse@jhuapl.edu

LtCol Ales MYNARIK
NATO JCBRN Defence COE
CZECH REPUBLIC
Email: mynarika@jcbrncoe.cz

Mr. Rick NEWELL
JFTC
POLAND
Email: rick.newell@jftc.nato.int

Mr. Jeppe NYLOKKE
IFAD TS A/S
DENMARK
Email: jeppe.nylokke@ifad.dk

Mr. Robbie PHILIPPS
Lockheed Martin Corporation
AUSTRALIA
Email: robbie.phillips@lmco.com

Mr. Marco PICOLLO
Finmecanica
ITALY
Email: marco.picollo@finmeccanica.com

Dr. LtCol (Ret) Dalibor PROCHAZKA
University of Defence
CZECH REPUBLIC
Email: dalibor.prochazka@unob.cz

Mr. Tomasz ROGULA
NATO Joint Force Training Centre
POLAND
Email: tomasz.rogula@jftc.nato.int

Dr. Martin ROTHER
IABG mbH
GERMANY
Email: rother@iabg.de

Mr. Angel SAN JOSE MARTIN
NATO ACT
UNITED STATES
Email: Angel.SanJoseMartin@act.nato.int

Maj Alfio SCACCIANOCE
NATO M&S CoE
ITALY
Email: mscoe.cde05@smd.difesa.it

LtCol Wolfhard SCHMIDT
JFTC
POLAND
Email: wolfhard.schmidt@jftc.nato.int

Mr. Barry SIEGEL
SPAWAR Systems Center – Pacific
UNITED STATES
Email: Barry.Siegel@navy.mil

Mrs. Louise SIMPSON
Thales
UNITED KINGDOM
Email: louise.simpson@uk.thalesgroup.com

Mr. Neil SMITH
UK MoD Dstl
UNITED KINGDOM
Email: nsmith@dstl.gov.uk

Mr. Per-Philip SOLLIN
Pitch Technologies AB
SWEDEN
Email: per-philip.sollin@pitch.se

Dr. Ralf STÜBER
CPA ReDev mbH
GERMANY
Email: stueber@supportgis.de

Capt Colin TIMMONS
Department of National Defence
CANADA
Email: colin.timmons@forces.gc.ca

Maj Dennis VAN DEN ENDE
Ministry of Defence
NETHERLANDS
Email: d.vd.ende@mindef.nl

Mr. Martin Dalgaard VILLUMSEN
IFAD TS A/S
DENMARK
Email: Martin.Villumsen@ifad.dk

Mr. Brian WARDMAN
Dstl Portsdown West
UNITED KINGDOM
Email: bwardman@dstl.gov.uk

Mr. Andrzej WNUK
Joint Warfare Centre
NORWAY
Email: andrzej.wnuk@jwc.nato.int

ADDITIONAL CONTRIBUTORS

Mr. Andy BOWERS
US Joint Staff J7
UNITED STATES
Email: francis.bowers@gdit.com

Mr. Brent MORROW
US Military Academy
UNITED STATES
Email: Brent.Morrow@usma.edu

Mr. Cory SAYLES
Lockheed Martin
UNITED STATES
Email: Cory.d.sayles@lmco.com

Mr. Roy SCRUDDER
The University of Texas at Austin
UNITED STATES
Email: roy.scrudder@arlut.utexas.edu

Mr. Dennis WILDE
European IAD Centre
UNITED STATES
Email: dennis.wilde@us.af.mil

Operational Concept Document (OCD) for the Allied Framework for M&S as a Service

(STO-TR-MSG-136-Part-III)

Executive Summary

NATO and nations use simulation environments for various purposes, such as training, capability development, mission rehearsal and decision support in acquisition processes. Consequently, Modelling and Simulation (M&S) has become a critical capability for the alliance and its nations. M&S products are highly valuable resources and it is essential that M&S products, data and processes are conveniently accessible to a large number of users as often as possible. However, achieving interoperability between simulation systems and ensuring credibility of results currently requires large efforts with regards to time, personnel and budget.

Recent developments in cloud computing technology and service-oriented architectures offer opportunities to better utilize M&S capabilities in order to satisfy NATO critical needs. M&S as a Service (MSaaS) is a new concept that includes service orientation and the provision of M&S applications via the as-a-service model of cloud computing to enable more composable simulation environments that can be deployed and executed on-demand. The MSaaS paradigm supports stand-alone use as well as integration of multiple simulated and real systems into a unified cloud-based simulation environment whenever the need arises.

NATO MSG-136 ("Modelling and Simulation as a Service – Rapid deployment of interoperable and credible simulation environments") investigated the new concept of MSaaS with the aim of providing the technical and organizational foundations to establish the *Allied Framework for M&S as a Service* within NATO and partner nations. The *Allied Framework for M&S as a Service* is the common approach of NATO and nations towards implementing MSaaS and is defined by the following documents:

- Operational Concept Document;
- Technical Reference Architecture (including service discovery, engineering process and experimentation documentation); and
- Governance Policies.

MSG-136 evaluated the MSaaS concept in various experiments. The experimentation results and initial operational applications demonstrate that MSaaS is capable of realizing the vision that M&S products, data and processes are conveniently accessible to a large number of users whenever and wherever needed. MSG-136 strongly recommends NATO and nations to advance and to promote the operational readiness of M&S as a Service, and to conduct required Science and Technology efforts to close current gaps.

This document describes the Operational Concept for the Allied Framework for MSaaS. The Operational Concept Document (OCD) describes the intended use, key capabilities and desired effects of the Allied Framework for M&S as a Service from a user's perspective.

Document de définition opérationnelle (OCD) du cadre allié de M&S en tant que service

(STO-TR-MSG-136-Part-III)

Synthèse

L'OTAN et les pays membres utilisent les environnements de simulation à différentes fins, telles que la formation, le développement capacitaire, l'entraînement opérationnel et l'aide à la décision dans les processus d'acquisition. Par conséquent, la modélisation et simulation (M&S) est devenue une capacité cruciale pour l'Alliance et ses pays membres. Les produits de M&S sont des ressources extrêmement précieuses ; il est essentiel que les produits, données et procédés de M&S soient facilement accessibles à un grand nombre d'utilisateurs aussi fréquemment que possible. Toutefois, l'interopérabilité entre les systèmes de simulation et la crédibilité des résultats ne sont pas encore acquises et nécessitent beaucoup de temps, de personnel et d'argent.

Les évolutions récentes du cloud informatique et des architectures orientées service offrent l'occasion de mieux utiliser les capacités de M&S afin de répondre aux besoins cruciaux de l'OTAN. La M&S en tant que service (MSaaS) est un nouveau concept qui inclut l'orientation service et la fourniture d'applications de M&S via le modèle « en tant que service » du cloud informatique, dans le but de proposer des environnements de simulation plus faciles à composer et pouvant être déployés et exécutés à la demande. Le paradigme du MSaaS permet aussi bien une utilisation autonome que l'intégration de multiples systèmes simulés et réels au sein d'un environnement de simulation dans le cloud, chaque fois que le besoin s'en fait sentir.

Le MSG-136 de l'OTAN (« Modélisation et simulation en tant que service (MSaaS) – Déploiement rapide d'environnements de simulation crédibles et interopérables ») a étudié le nouveau concept de MSaaS afin de fournir les bases techniques et organisationnelles permettant d'établir le « cadre allié de M&S en tant que service » au sein de l'OTAN et des pays partenaires. Le cadre allié de M&S en tant que service est la démarche commune de l'OTAN et des pays visant à mettre en œuvre la MSaaS. Il est défini dans les documents suivant :

- Document de définition opérationnelle ;
- Architecture de référence technique (incluant la communication du service, le processus d'ingénierie et la documentation d'expérimentation) ; et
- Politiques de gouvernance.

Le MSG-136 a évalué le concept de MSaaS au moyen de diverses expériences. Les résultats d'expérimentation et les premières applications opérationnelles démontrent que la MSaaS est capable de rendre les produits, données et processus de M&S commodément accessibles à un grand nombre d'utilisateurs, quels que soient l'endroit et le moment où le besoin s'en fait sentir. Le MSG-136 recommande vivement à l'OTAN et aux pays membres de faire progresser et d'améliorer l'état de préparation opérationnelle de la M&S en tant que service et de mener les travaux de science et technologie requis pour combler les lacunes actuelles.

Ce document décrit le concept opérationnel du cadre allié de la MSaaS. Le document de définition opérationnelle (OCD) indique l'utilisation prévue, les capacités clés et les effets souhaités du cadre allié de M&S en tant que service, du point de vue de l'utilisateur.

Chapter 1 – INTRODUCTION

1.1 BACKGROUND AND KEY DRIVERS

Emerging cloud computing technology and various NATO and National policies were the key drivers for the NATO Modelling and Simulation Group (NMSG) to investigate the potential effect for Modelling and Simulation. The NMSG Specialist Team MSG-131 conducted a one year study into "Modelling and Simulation as a Service (MSaaS): New Concepts and Service-Oriented Architectures" [1].

Based on a survey of existing MSaaS case studies, MSG-131 concluded that service-based approaches can contribute towards more efficient Modelling and Simulation (M&S). MSG-131 recommended that investigation of MSaaS should be conducted in more detail. This resulted in the establishment of Research Task Group MSG-136 ("Modelling and Simulation (M&S) as a Service (MSaaS) – Rapid deployment of interoperable and credible simulation environments") with a 3-year program of work from 2014 to 2017.

NATO and Partners face challenges regarding training and exercises: current and future operations are multi-national in nature; the missions and the systems are becoming more complex and require more detailed preparation and rapid adaptation to changing circumstances. At the same time, opportunities for (live) training and exercises for distant partners are reduced due to complexity and available resources and limited time span between political decision making and mission execution.

Simulation has now become an essential tool to meet the needs of combined joint forces not only for training, but also for support to operations, mission rehearsal, procurement and capability developments.

Improvements in M&S technical capabilities and reduced costs will enable more effective use of these tools across nations and organizations. The MSG-136 research has developed the MSaaS Reference Architecture and procedures. Specific solutions and recommendations will be the baseline for an improved M&S capability for NATO and its Partners.

It is anticipated that future military capabilities, including training, mission planning and decision making will be provided through increased use of M&S. However, there are currently two main barriers which are the perceived cost and time taken to compose and develop simulation systems. Furthermore, limited credibility resulting from unknown validity and *ad hoc* processes is still a serious problem.

M&S products are highly valuable to NATO and military organizations, and it is essential that M&S products, data and processes are conveniently accessible to a large number of users as often as possible. Therefore, a new "M&S ecosystem" is required where M&S products can be more readily identified and accessed by a large number of users to meet their specific requirements. 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 combination of service-based approaches hereby referred to as "Modelling and Simulation as a Service" (MSaaS) is considered to be a very effective approach for composing next generation simulation systems. NATO MSG-136 was tasked to investigate, propose and evaluate standards, agreements, architectures, implementations, and cost-benefit analysis for incremental implementation of a permanently available, flexible, service-based eco-system to provide more cost effective availability of M&S products, data and processes to a large number of users on-demand.

The NATO M&S Master Plan [2] identified several gaps and defined five main objectives:

- Establish a Common Technical Framework;

- Provide Coordination and Common Services;
- Develop Models and Simulations;
- Employ Simulations; and
- Incorporate Technological Advances.

The Allied Framework for MSaaS as defined by this document seeks to address these objectives. Regarding the use of M&S in support of military training the NATO M&S Gap Analysis Report [3] and the findings of NMSG ET-039 [4] detail these objectives in accordance with the NATO M&S Standards Profile (NMSSP) document [5].

1.2 PURPOSE OF THE OPERATIONAL CONCEPT DOCUMENT

The purpose of the Operational Concept Document (OCD) for the Allied Framework for M&S as a Service (MSaaS) is to inform relevant stakeholders how the framework will function in practice. The capabilities and key characteristics of the proposed framework are included in the operational concept as well as the interactions of the users.

The OCD provides a clear and concise documentation to the stakeholders, especially for reference and guidance for all parties, to ensure a common understanding of the Allied Framework for M&S as a Service. A clear understanding of how stakeholders will interact with the system and how they interact with each other with regards to the system is a crucial function of the OCD. Specifically, the main goals of the OCD are to enable the operational stakeholders to evolve knowledgeably from their current and inadequate operational situation to the new operational situation. It also serves as a platform for stakeholders to collaboratively adapt their understanding of the systems operation as new developments, requirements or challenges arise. Therefore, the OCD is written in the common language of all interested parties.

1.3 IDENTIFICATION

The framework described by this OCD is identified as follows:

- Name: Allied Framework for M&S as a Service
- Abbreviation: M&S as a Service (MSaaS)

1.4 DEFINITIONS

The Allied Framework for M&S as a Service is the common approach of NATO and Nations towards implementing MSaaS and is defined by the following documents:

- **Operational Concept Document (OCD):** The OCD describes the intended use, key capabilities and desired effects of the Allied Framework for M&S as a Service from a user's perspective.
- **Technical Reference Architecture and Associated Volumes:** The Technical Reference Architecture describes the architectural building blocks and patterns for realizing MSaaS capabilities.
- **Governance Policies:** The MSaaS Governance Policies identify MSaaS stakeholders, their relationships and provide guidance for implementing and maintaining the Allied Framework for M&S as a Service as a persistent capability.

The documents mentioned above define the blueprint for individual organizations to implement MSaaS. However, specific implementations may be different for each organization.

This document uses key definitions as provided by the Allied M&S Publication (AMSP) on the "Allied Framework for Modelling and Simulation (MSaaS) Governance Policies".

"An **M&S service** is a specific M&S-related capability delivered by a provider to one or more consumers according to well defined contracts including Service Level Agreements (SLA) and interfaces." [6]

"**M&S as a Service (MSaaS)** is an enterprise-level approach for discovery, composition, execution and management of M&S services." [6]

"An **MSaaS Implementation** is the specific realization of M&S as a Service by a certain organization as defined in the Operational Concept Document. An MSaaS Implementation includes both technical and organizational aspects." [6]

"An **MSaaS Solution Architecture** is the architecture of a specific MSaaS implementation and is derived from the Operational Concept Document and the Technical Reference Architecture." [6]

Chapter 2 – ALLIED FRAMEWORK FOR M&S AS A SERVICE

This chapter defines the vision of an Allied Framework for M&S as a Service. Based on the overarching vision of NATO and the NMSG, the MSaaS Vision Statement and Goals are derived. The Allied Framework for M&S as a Service is illustrated and an incremental implementation strategy is presented.

2.1 VISION STATEMENT AND MISSION

The North Atlantic Treaty Organization (NATO) Modelling and Simulation Master Plan (NMSMP) defines the following vision regarding M&S:

NMSMP Vision
"Exploit M&S to its full potential across NATO and the Nations to enhance both operational and cost effectiveness." [2]

The MSaaS Vision Statement defines from a user's point of view the desired end-state of a future operational M&S environment:

MSaaS Vision Statement
M&S products, data and processes are conveniently accessible and available on-demand to all users in order to enhance operational effectiveness.

2.2 MSAAS GOALS

To achieve the MSaaS Vision Statement the following MSaaS goals are defined:

1) **To provide a framework that enables credible and effective M&S services:** MSaaS aims to provide a common, consistent, seamless and fit for purpose M&S capability to the user that is reusable and scalable in a distributed environment.
2) **To make M&S services available on-demand to a large number of users:** MSaaS aims to offer the users the ability to get timely access to services through scheduling and computing management. Users can dynamically provision computing capabilities, such as server time and network storage, as needed, automatically without requiring human interaction. Quick deployment of the customer solution is possible since the used services are already installed, configured and on-line.
3) **To make M&S Services available in an efficient and cost-effective way:** MSaaS aims to achieve convenient short set-up time and low maintenance costs for the community of users. MSaaS offers the service consumers the ability to increase efficiency by automating efforts.
4) **To provide the required level of agility to enable convenient and rapid integration of capabilities:** MSaaS offers the users the ability to evolve systems by rapid provisioning of resources, re-configuration, configuration management, deployment and migration of legacy systems. It is also tied to business dynamics of M&S that allow for the discovery and use of new services beyond the users' current configuration.

2.3 OPERATIONAL CONCEPT OF THE ALLIED FRAMEWORK FOR MSAAS

The MSaaS Operational Concept Document (OCD) describes the intended use, key capabilities and desired effects of the Allied Framework for M&S as a Service from a user's perspective.

The Allied Framework for M&S as a Service enables:

1) The community of users to discover new opportunities to train and to work together.
2) Users to enhance their operational effectiveness, saving costs and effort in the process. By pooling individual user's requirements and bundling individual requests in larger procurement efforts, the position of buying authorities against industrial providers is strengthened.
3) M&S services that are readily available on-demand and deliver a choice of applications in a flexible and adaptive manner. It offers advantages over the existing stove-piped M&S paradigm in which the users are highly dependent on a limited amount of industry partners and subject matter experts.

The Allied Framework for MSaaS provides the linking element between M&S services that are provided by a community of stakeholders to be shared and the users that are actually utilizing these capabilities for their individual needs (see Figure 2-1).

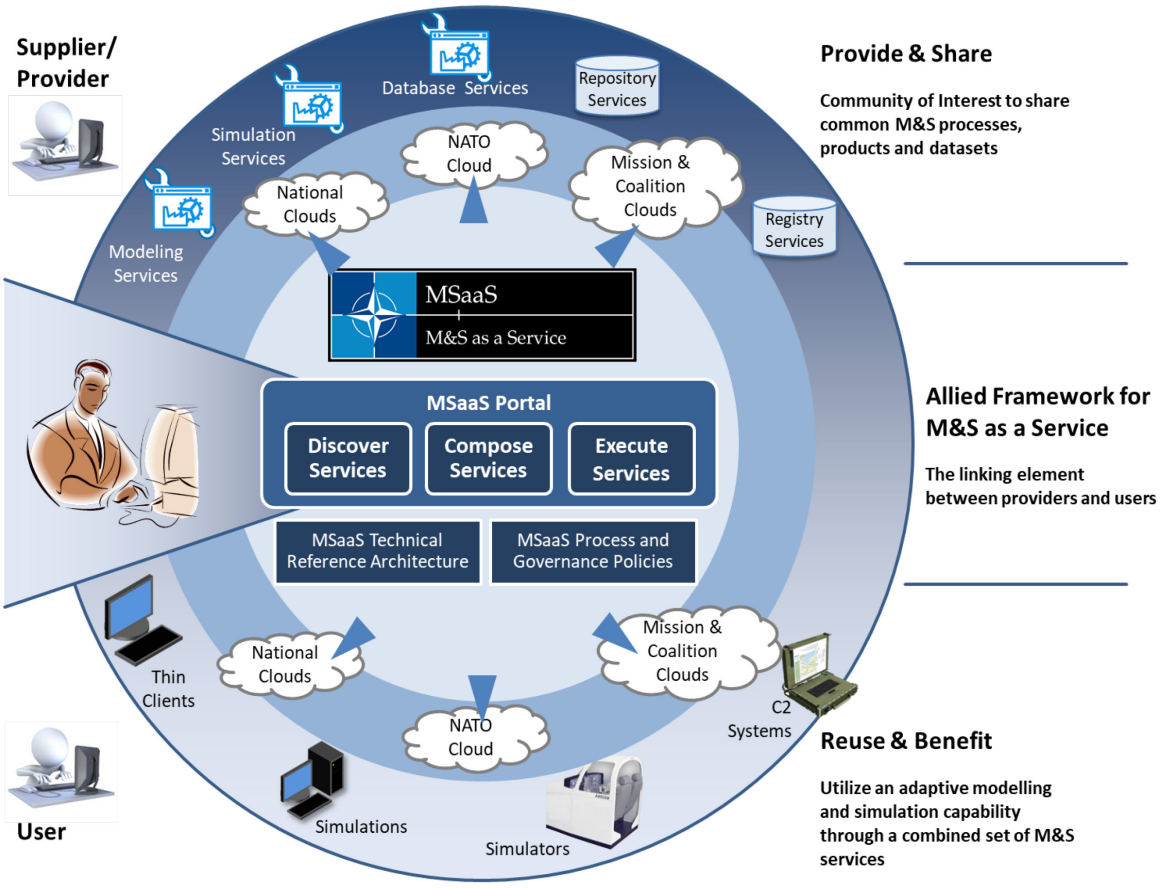

Figure 2-1: Operational Concept of the Allied Framework for M&S as a Service.

The Allied Framework for MSaaS defines the user facing capabilities (Front-end) and underlying technical infrastructure (Back-end). The Front-end provides access to a large variety of M&S capabilities from which the users are able to select the services that best suit their requirements, and track the experiences and lessons learned of other users.

The users are able to discover, compose and execute M&S services through a Front-end (MSaaS Portal), which is the central access point that guides them through the process. The key activities supported by the Allied Framework for MSaaS and made available to the users through the MSaaS Portal (see Figure 2-1) are:

- **Discover:** To facilitate reuse of existing resources the Allied Framework for MSaaS provides a mechanism for users to search and discover M&S services and resources (e.g., data, services, models, federations, and scenarios). A registry is used to catalogue available content from NATO, nations, industry and academic organizations. This registry provides useful information on available services and assets in a manner that the user is able to assess their suitability to meet a particular requirement (i.e., user rating, requirements, simulation specific information, and verification and validation information). The registry also points to a repository (or owner) where that simulation service or asset is stored and can be obtained, including business model information (i.e., license fees, pay per use costs).

  Figure 2-2 illustrates the concept of distributed registries being able to search and discover simulation assets from various different repositories (i.e., those from industry, academic, NATO or national organizations).

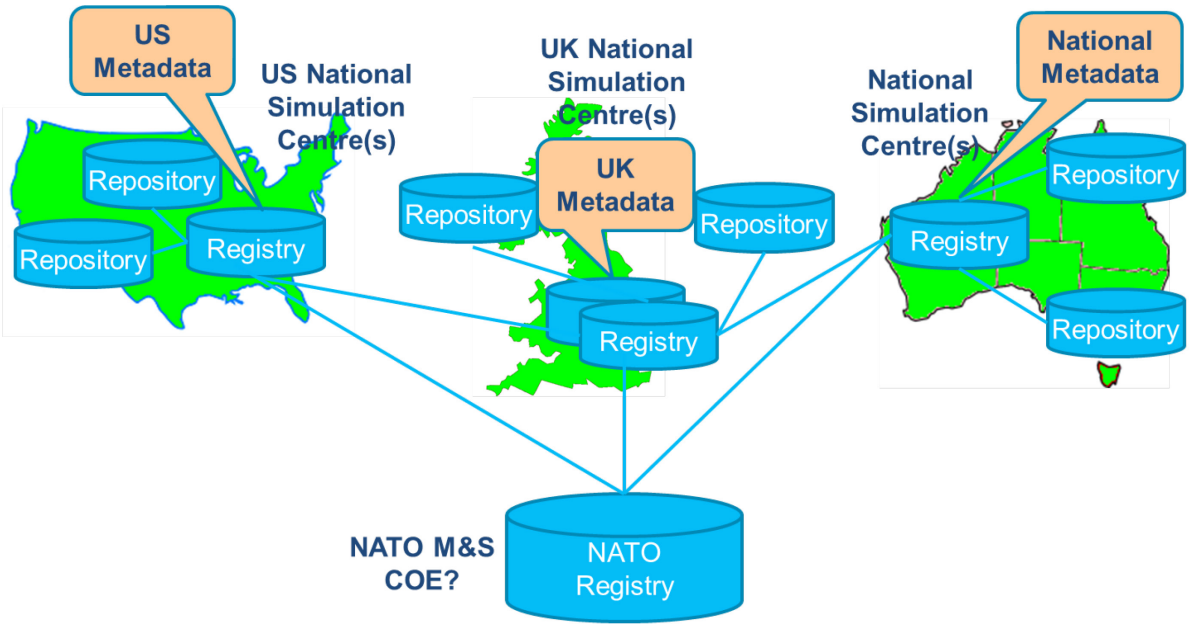

Figure 2-2: Sharing of Registry Content Across Nations.

Figure 2-3 emphasizes that registries also have a mechanism of sharing information between themselves in a manner that allows them to expose publicly available information and prevent private information from being shared (e.g., for security or confidentiality reasons). It is expected that there will be different levels of public and private access to such information given the organizational or user agreements and access rights (i.e., international information exchange agreements, personal security clearance). A NATO registry could act as broker between NATO and national organizations information exchange.

- **Compose:** The Allied Framework for MSaaS provides the ability to compose discovered services to perform a given simulation use case. Initially it is envisaged that simulation services will be composed through existing simulation architectures and protocols and can be executed on-demand (i.e., with no set up time). In the longer term, distributed simulation technology will evolve, enabling further automation of discovery, composition and execution than is possible today.
- **Execute:** The Allied Framework for MSaaS provides the ability to deploy and execute the composed services automatically on a cloud-based or local computing infrastructure. The automated deployment and execution allows to exploit the benefits of cloud computing (e.g., scalability,

resilience). Once deployed and executed the M&S services can be accessed on-demand by a range of users (Live, Virtual, Constructive) directly through a simulator (e.g., a flight simulator consuming a weapon effects service), through a C2 system (e.g., embedded route planning functionality that utilizes a route planning service) or may be provided by a thin client or by a dedicated application (e.g., a decision support system utilizing various services like terrain data service, intelligence information service etc.). The execution services support a range of business models and are able to provide data relevant to those models (i.e., capture usage data for a pay per use business model).

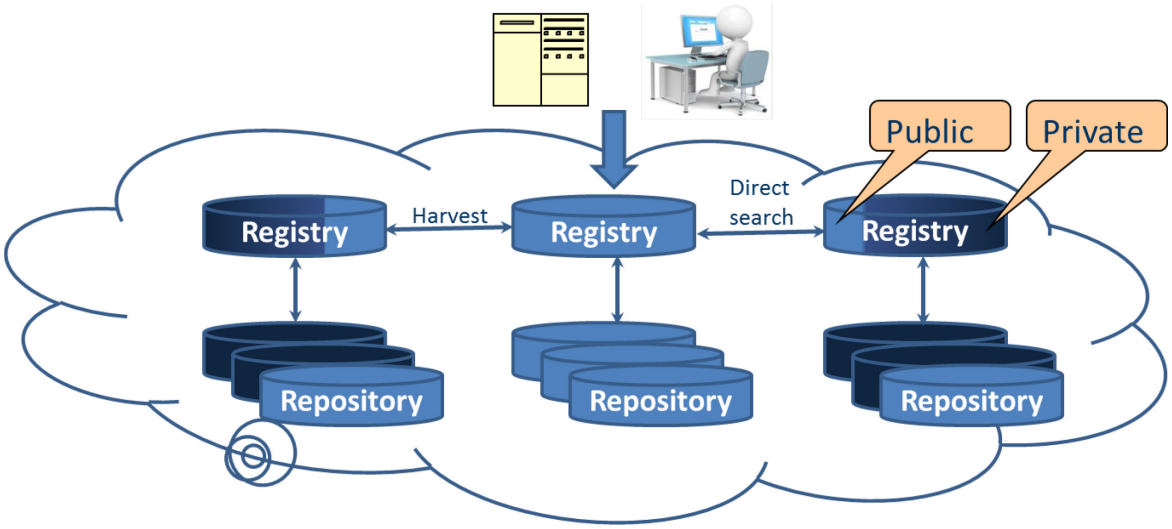

Figure 2-3: Secure Registry Information Sharing.

The Allied Framework for MSaaS provides key elements for realizing the activities mentioned above and for achieving the overall MSaaS goals:

- **MSaaS Technical Reference Architecture:** The MSaaS Technical Reference Architecture provides the architectural foundation (i.e., metadata approaches, interoperability protocols, architectural building blocks and patterns) to enable the Allied Framework for MSaaS to provide Discovery, Composition and Execution of services. In addition, the MSaaS Technical Reference Architecture provides engineering processes and best practice guides for setting up service-based simulation environments.
- **MSaaS Process and Governance Policies:** Identifies MSaaS stakeholders and their relations and provides guidance for implementing and maintaining the Allied Framework for M&S as a Service. The MSaaS Governance Policies define the (long-term) governance of the Allied Framework for M&S as a Service, e.g., compliance criteria for new services joining the framework, guidelines and rules for specifying and documenting services, etc.

The Allied Framework for MSaaS is the linking element between service providers and users by providing a coherent and integrated capability with a technical Reference Architecture, recommendations and specifications for Discovery, Composition and Execution of Services and defines necessary processes and governance policies.

2.4 STAKEHOLDERS AND RELATIONSHIPS

This chapter provides an overview of the stakeholders of the Allied Framework for M&S as a Service and their individual relationships. The role definitions are aligned with the descriptions available in the NATO M&S Master Plan [2].

The MSaaS stakeholder roles that are identified in the Allied Framework for MSaaS are shown in Figure 2-4.

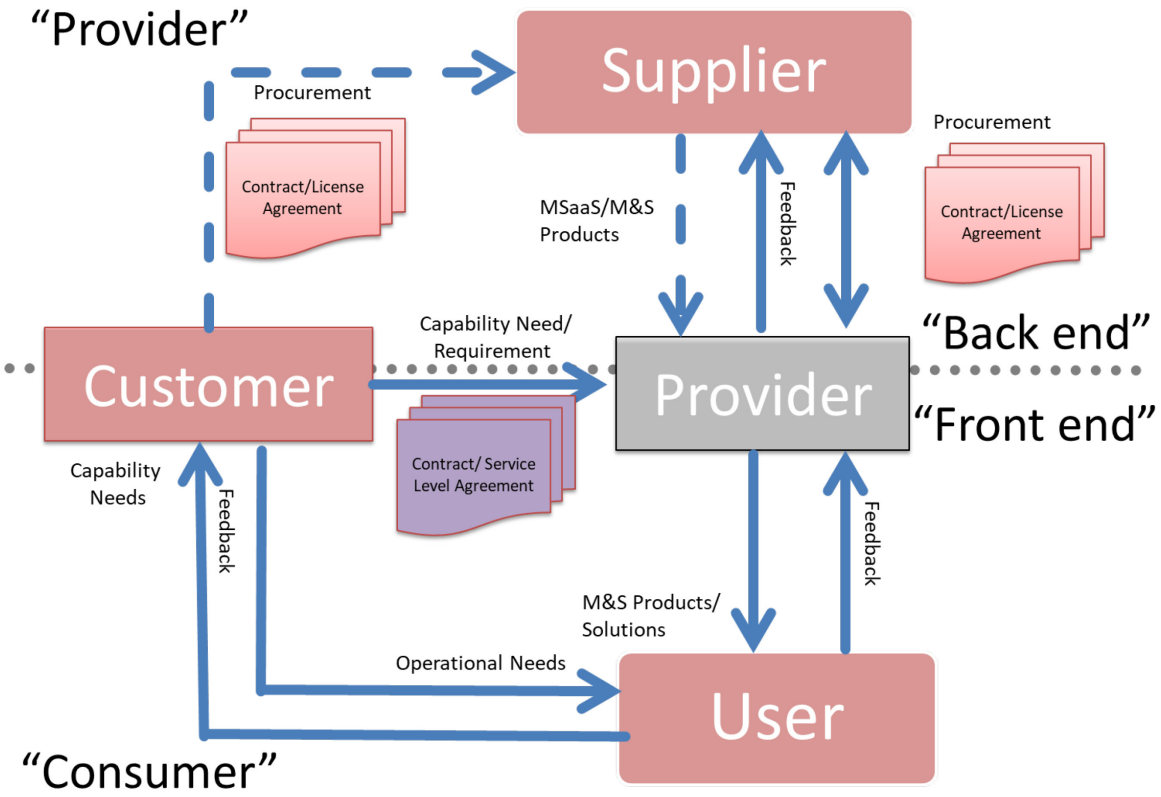

Figure 2-4: MSaaS Stakeholder Roles in the Allied Framework for MSaaS.

The stakeholders identified in Figure 2-4 represent generic roles that are required for implementing MSaaS as a persistent capability. Each nation or organization that implements MSaaS has to map these generic roles to its specific organizational structures. Depending on the actual organizational structures, it may be the case that some of the stakeholders identified in Figure 2-4 are actually represented by the same organizational entity.

At the top-level, Figure 2-4 distinguishes between Providers and Consumers. This is not a sharp distinction but is intended as a rough indication of whether a stakeholder is considered primarily as being a provider of services or a consumer of services. Note that Figure 2-4 does not show an organizational boundary. The purpose of a missing organizational boundary is to stress the flexibility and applicability of the concept. Depending on the actual organization the supplier role may be either outside or inside the organization. The *front end* covers the user-facing aspects of MSaaS, while the *back end* covers the procurement and development efforts to realize MSaaS.

The individual stakeholders are explained in the following sections.

2.4.1 Customer

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

2.4.2 Provider

In accordance with Customer SLAs the MSaaS Provider makes M&S products and services (including integrated services such as executable simulations) available to Users of the Allied Framework for MSaaS. The MSaaS Provider needs to manage and maintain a core set of services in order to meet SLAs. This will include the use of registry and discovery services to maintain visibility and availability of M&S products, 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:

- Ensuring that M&S products and services have been formally verified by Suppliers;
- The composability and interoperability between M&S products and solutions; and
- Monitoring and measuring the usage of the MSaaS capabilities, and is responsible for billing according to license agreements.

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

2.4.3 User

The MSaaS User is the consumer of MSaaS products and services. The User may take responsibility for the composition of M&S products and services in accordance with Customer requirements.

There are different types of User that can be considered in the context of the Allied Framework for MSaaS. Examples of these can include:

- Operational End Users who define their capability needs to the Customer and who benefit from M&S products and services, e.g., primary training audience in Command Post Exercises (CPX) or Computer Assisted Exercises (CAX); and
- Simulation Operators who use MSaaS products and services to provide simulation capabilities and applications to the Operational End User, e.g., training center personnel and secondary training audience in a CPX/CAX.

In order to provide more clarification relevant to the examples given above the primary training audience would be a Command Post (CP) at the Brigade level. This audience consists of Commanders and Staff Officers who benefit from using simulated scenarios, e.g., to have an operational picture, to obtain orders, feedbacks and/or to receive events which they need to respond to. This audience is not responsible for the direct configuration of M&S products and solutions. The training center personnel are responsible for directly configuring the scenario aimed at training the Operational End User, by creating events and using models based on M&S products and solutions available from the Allied Framework for MSaaS. Furthermore, there could be other users of M&S products and solutions, such as a secondary training audience (e.g., role players) who configure or interact with constructive simulation tools to provide the behavior of lower level force units, e.g., squad, platoons.

The User (e.g., Operational End User) is responsible for providing data and feedback on performance and functionality of the Allied Framework for MSaaS to the Customer.

2.4.4 Supplier

MSaaS Suppliers develop and provide M&S products and solutions. This includes maintaining repositories of M&S products and making these available to MSaaS providers as part of the Allied Framework for

MSaaS either via a product procurement or license agreement. Examples of Suppliers include large defence contractors, small and medium enterprises and academic institutions, in addition to Government organizations.

2.5 RELATIONSHIPS

The MSaaS concept requires negotiation between Customers, Suppliers, Service Providers and Users.

2.5.1 Customers

The Customer will assist the User by capturing the capability needs based on the operational needs, and breaking these down in technical requirements.

The Customer needs to consider the use of MSaaS capabilities available from the Allied Framework for MSaaS, typically 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 to Users as part of the Allied Framework for MSaaS.

The Customer will engage with Users to capture feedback on performance and functionality of the Allied Framework for MSaaS as part of verifying and validating M&S products and services.

2.5.2 Providers

Service Providers will engage with Suppliers to acquire and integrate M&S products in accordance with SLAs agreed with Customers. The resultant products and services will then be made available for composing services to Users who have been verified for access. Providers will engage with Users and Customers to capture any feedback on the deployment, integration and execution of M&S products and services, and where relevant provide information back to Suppliers.

2.5.3 Users

The User defines the capability needs to the Customer and will consume M&S products and services in accordance with the SLA between the Customer and the Service Provider. Following execution of the M&S products and services the User (e.g. Operational End User) shall inform the Customer on performance and functionality of the Allied Framework for MSaaS so that the Customer in conjunction with the Provider can verify and validate M&S products and services.

2.5.4 Suppliers

The Supplier will respond to requests from service Providers and Customers for the provision of M&S products and services. Any subsequent delivery of M&S products and services will require a contract or license agreement between the Supplier and service Provider/Customer. The Supplier will capture feedback from the service Provider on delivered M&S products and services.

2.5.5 Example of Interaction Between Stakeholders

The interaction between the various stakeholders is illustrated in the following example:

1) Consumer and User collect operational needs;
2) User states Capability Needs to Customer (e.g., requirements for simulation support for training and/or exercises);

3) Customer makes agreement about capabilities with Provider;
4) Provider deals with Supplier to service Customer cfm agreement and makes a contract with Supplier;
5) Customer deals with Suppliers License agreement;
6) Provider opens / sets up Environment for User;
7) User does training/exercise in Simulation;
8) User provides feedback to Customer and Provider; and
9) Provider provides feedback to Supplier.

The above example is illustrative and does not cover situations that need special attention.

2.6 INTEROPERABILITY OF ALLIED AND NATIONAL MSAAS IMPLEMENTATIONS

It is assumed that multiple MSaaS implementations will exist:

- MSaaS implementation on NATO level;
- MSaaS implementations on national level;
- Mission-specific MSaaS implementations; and
- MSaaS implementations on different security levels (e.g., NATO UNCLASSIFIED, NATO SECRET).

The objective of the Allied Framework for MSaaS is to create interoperability between these implementations and to make sure that different MSaaS implementations can interoperate with each other.

2.7 APPLICATION AREAS AND EXAMPLE USE CASE

The Allied Framework for M&S as a Service supports all application areas as defined by the NATO Modelling and Simulation Master Plan [2]:

- Training (collective training, individual training);
- Support to Operations Planning;
- Capability Development;
- Mission Rehearsal; and
- Procurement/Acquisition.

Examples for these application areas and potentially involved stakeholders are given in Annex A.

Figure 2-5 is an example of general steps to implement an MSaaS operational concept in alignment with the Distributed Simulation Engineering and Execution Process (DSEEP). The example uses a training-oriented use case, but it is important to note that MSaaS is not limited to training but can be used for all application areas.

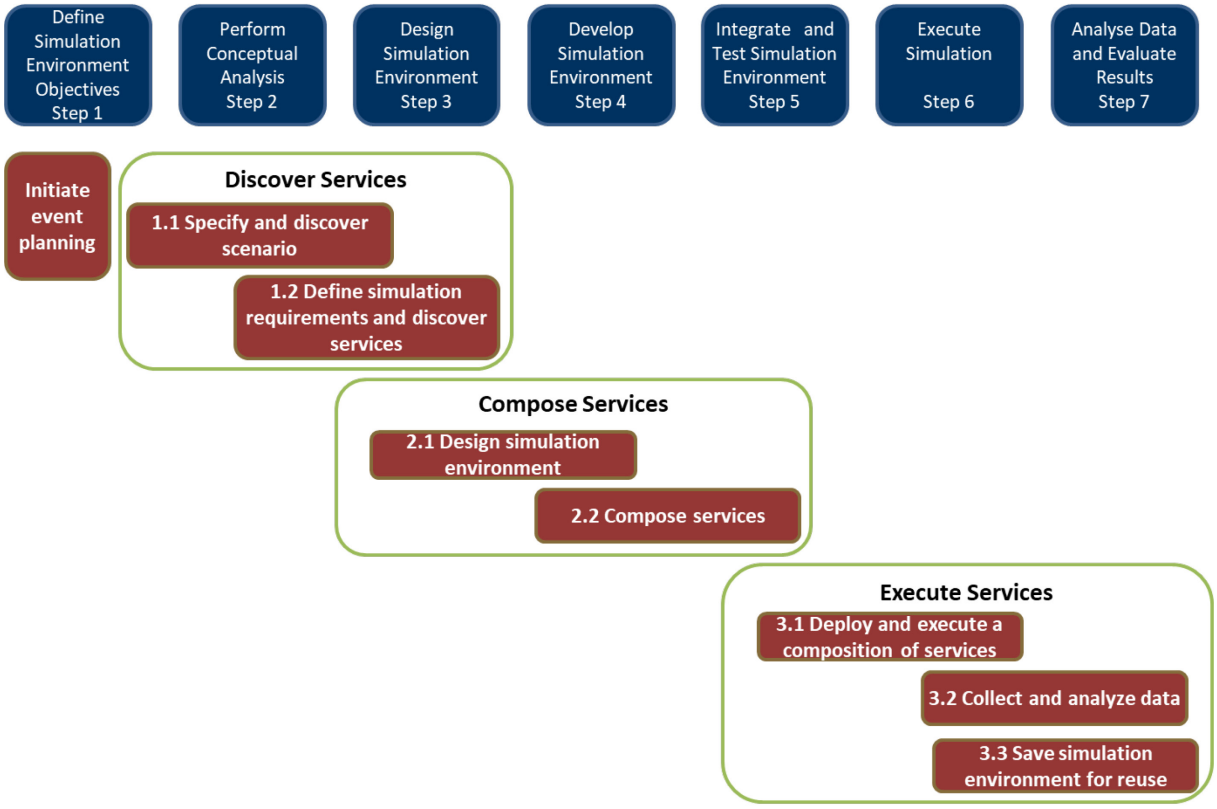

Figure 2-5: Alignment of Activities with DSEEP Steps.

Discover Services:

- Activity 1.1 Specify and discover scenario.
- Activity 1.2 Define simulation requirements and discover services.

Compose Services:

- Activity 2.1 Design simulation environment.
- Activity 2.2 Compose services.

Execute Services:

- Activity 3.1 Deploy and execute a composition of services.
- Activity 3.2 Collect and analyze data.
- Activity 3.3 Save simulation environment for reuse.

A further description of the process and associated activities a user might execute is given in the following sections. For the following activities and use cases in Annex A, it is assumed that the following supporting services and infrastructure are available to the user:

- Availability of a registry with information about available M&S services and capabilities.
- Availability of a repository with access to the actual M&S services and capabilities.
- Availability of an MSaaS Portal as a central Front-end providing discovery, composition and execution services.

- Availability of networking and hardware infrastructure (Cloud provider, local hardware, network) on which to execute the simulation services.

2.7.1 Initiate Event Planning

The first activity executed by a user is to initiate the event planning. This includes creating templates, etc. in the MSaaS Portal and assigning tasks to people.

Example Workflow:

1) User logs in to MSaaS Portal and creates a new event (including name, date, etc.). An event may be an exercise, an experiment, etc.
2) User assigns roles to persons (like event director, support staff, etc.).
3) User specifies event objectives.
4) User specifies a scenario. The user may choose from different options:
   a) Option A: Select scenario/vignette from a library.
   b) Option B: Select and adapt an existing scenario/vignette.
   c) Option C: Develop a new scenario/vignette.
5) User specifies event partners (e.g., other nations, organizations).

2.7.2 Discover Services

2.7.2.1 Activity 1.1: Specify and Discover Scenario

After the event was initiated the user needs to specify the scenario and (if possible) discover and select a scenario from a repository.

Example Workflow:

1) User specifies a scenario. The user may choose from different options:
   a) Option A: Select scenario/vignette from a library.
   b) Option B: Select and adapt an existing scenario/vignette.
   c) Option C: Develop a new scenario/vignette.

2.7.2.2 Activity 1.2: Define Simulation Requirements and Discover Services

After the event was initiated the user defines the simulation requirements (based on the original event objectives) and discovers appropriate services.

Example Workflow:

1) The user (e.g., a dedicated simulation engineer) logs in to the MSaaS Portal and specifies simulation requirements to achieve the event objectives.
2) User identifies required networks and connections (e.g., national networks, coalition networks).

3) User searches MSaaS Portal for available simulation services (local, remote). The set of services available to any specific user will be limited by various constraints (licenses, export regulations, etc.).
4) User discovers most appropriate services. The service descriptions available in the MSaaS Portal for each service include information about purpose of a service, runtime constraints, required input data, etc. of a service. As a service may be dependent on other services, the MSaaS Portal notifies the user of any such dependencies.

2.7.3 Compose Services

In this example the assumption is that the simulation design and all selected services are executable, interoperable, and composable and therefore require no iteration by the user or provider.

2.7.3.1 Activity 2.1: Design Simulation Environment

Once the user has defined the simulation requirements and discovered appropriate services for implementing the simulation environment, the simulation environment is designed and the services are composed to be executed together.

Example Workflow:

1) User selects services for the specific event and if required configures these services. An example for configuring a service is to enter the Order of Battle (ORBAT) that was initially described on a set of PowerPoint slides into an ORBAT service.
2) The user stores all configuration items (services, versions, configuration data, additional datasets, etc.) in the MSaaS Portal.

2.7.3.2 Activity 2.2: Compose Services

Based on the simulation environment design and the selected services the actual composition (integration) of all parts happens.

Example Workflow:

1) User initiates instantiation of simulation environment in MSaaS Portal. The user is able to see the current structure and topology of the simulation environment, and can add additional services as required. Behind the scenes (i.e., invisible to the user) the simulation environment is composed automatically. This includes all necessary middleware and infrastructure based on the selected services and the simulation environment design.
2) User does verification and validation of the simulation environment. An example is to verify that the ORBAT information was correctly transferred from the original PowerPoint slides into the ORBAT service.

2.7.4 Execute Services

In this example the assumption is that the simulation environment design and service composition are finalized and available in the MSaaS Portal.

2.7.4.1 Activity 3.1: Deploy and Execute a Composition of Services

Shortly before the actual start of the event, the service composition is deployed to an appropriate computing infrastructure and all services are executed. As a result, the simulation environment is up and running, ready to support the user's event.

Example Workflow:

1) User logs in to MSaaS Portal, selects the event and starts the composition. The MSaaS Portal automatically provisions the required infrastructure.
2) Through the MSaaS Portal the user can monitor and control the simulation event. The user may start/stop/pause/etc. the simulation at any time.
3) The simulation execution is supervised and monitored by the MSaaS infrastructure and middleware. Through the MSaaS Portal the user can monitor the health of the simulation environment. Specific events (like unavailability of a service) will trigger a notification to the user (e.g., via email).

2.7.4.2 Activity 3.2: Collect and Analyze Data

During the actual simulation execution raw data is collected, aggregated and made available to the user for analysis purposes. This can be done by inclusion of a data-analysis service.

Example Workflow:

1) The user logs in to the MSaaS Portal and has access to all data collected during simulation execution.
2) The user starts an After Action Review service that allows him to playback the simulation execution and to give an outbrief to the training audience.

2.7.4.3 Activity 3.3: Save Simulation Environment for Reuse

After the actual event (e.g., exercise) the user saves artifacts for reuse in future events and identifies observations and recommendations for future events.

Example Workflow:

1) The user logs in to the MSaaS Portal and can archive simulation results.
2) The user can archive specific service compositions or the entire simulation environment for reuse.
3) User provides feedback via the MSaaS Portal on various aspects of the user experience (validate if simulation environment (= composition of services) met requirements, observations, shortfalls, errors, etc.)

2.8 IMPROVEMENTS, BENEFITS, RISKS AND CHALLENGES

Implementing the Allied Framework for M&S as a Service will result in various benefits and improvements for the different stakeholders. However, stakeholders that will implement the proposed concept into their organizations will also face risks and some major challenges. This section summarizes these improvements, benefits, and risks. More information may be found in Ref. [1], Chapter 2, Section 2.6.

2.8.1 Improvements and Benefits

MSaaS has the capability to deliver various benefits to all different stakeholders that interact within the framework. In this section the possible improvements and benefits to the stakeholders are described.

MSaaS will:

1) Increase operational effectiveness; and
2) Increase efficiency.

2.8.1.1 Increase Operational Effectiveness

- **Streamlined processes:** Compared to traditional systems, MSaaS will streamline the processes and organize deployment of M&S capabilities more efficiently. While improved deployment is achieved through use of virtualization and cloud technologies, streamlined processes are anticipated as a result of closer cooperation between NATO and nations with regards to sharing of M&S resources.
- **Greater accessibility of M&S services from remote locations:** The MSaaS concept provides the user with opportunities to access M&S services that are not physically owned or located in the area of operations. In this way, the concept can increase the availability of services on remote locations.
- **Increased efficiency and productivity in training:** Due to the increased access to a larger variety of M&S services, it will be possible to create and use more complex and complete simulation services. This will contribute to an increase in the efficiency and productivity of simulated training sessions.
- **Improved quality:** The MSaaS Portal creates transparency about existing services and thus supports selecting the best possible service for a specific user requirement. In addition, reusing services and avoiding duplication of efforts will lead to higher-quality services.

2.8.1.2 Increase Efficiency

- **Reduced manpower requirements:** As a result of the automated processes (driven by cloud-based technologies and current deployment techniques), the personnel requirements on the end of the service consumer can be significantly lowered compared to the current situation. Since more services are available and spread around in a community of interest, more services can be accessed than before, some of these services are developed for e.g., the EXCON organization to be more efficient and support them to produce HICON/LOCON products.
- **Reduced reliance on SMEs and available expertise:** In the MSaaS concept, a lot of the required knowledge and expertise required to deploy simulations nowadays will be provided as a service. Therefore, reliance on SMEs can be significantly reduced.
- **Increased reuse opportunities:** MSaaS is about sharing the available M&S resources with the MSaaS community. By pooling these resources and providing them as a service to other stakeholders within the framework, the opportunities for reuse will be increased.
- **Reduced duplication of effort:** The MSaaS concept can reduce the duplication of effort by reusing common and consistent products and datasets as a result of pooling M&S products and data resources. Computing resources are pooled to serve multiple consumers concurrently. Different physical and virtual resources are dynamically assigned and reassigned according to consumer demand.
- **Reduced cost of ownership:** While the MSaaS concept removes the necessity for actual physical ownership of an M&S service, the cost of ownership will most likely be reduced.

- **Single point of access to M&S services:** The MSaaS framework provides a single point of access (e.g., through the MSaaS Portal) for the users. Each user is required to login into the MSaaS framework only once (single sign-on) and may access all resources permitted by his role.
- **Provisioning of M&S resources during runtime:** When running a federation of services, the system should allow to use new services or discard old ones, during runtime, without any disruption nor downtime in the system.
- **Leverage benefits of cloud computing:** MSaaS allows leveraging benefits of cloud computing, like scalability, resilience, etc.

2.8.2 Risks

The following general (i.e., not defence-specific) risks associated with service-based M&S approaches have been identified:

- Managing security, privacy, accountability, risk and trust become more complex in a distributed, heterogeneous environment with multiple service owners.
- Advanced aspects of composability of M&S services are still an open area of research (e.g., service discovery, service binding).
- Availability of sufficient network connections (in terms of bandwidth, latency, etc.)
- Dependency on network connections makes M&S applications vulnerable to network effects out of the control of an M&S user.
- Adapting existing M&S applications with a service interface or for hosting in the cloud may be complex and/or costly. Not everything fits in the cloud, especially if it hadn't been designed for the cloud.
- Non-localized control over consumed services creates a dependency and reliance on a service provider to fulfil their service level agreements and removes the possibility of manually modifying the service should the provider not do so.
- If a composed MSaaS service is validated for some use, updates to individual services may require re-validation. Mitigating this requires well defined service management and governance to allow service users to continue using validated services while newer updates go through the validation process.

In addition to these general risks, there are also several (perceived) defence-specific risks:

- Poor performance of network infrastructure available to military users, especially those deployed, may make access to and use of M&S services difficult or impossible.
- Dependency on remote infrastructure and services increases vulnerability in front-line / combat situations and makes local fallback options and backup systems necessary, thus cancelling out the major advantages of MSaaS for these situations.
- Adaptation of existing software is needed (e.g., replace internal weapon effects calculation of a simulation system with an interface to a service providing the same functionality). This may prove difficult or impossible in the case of COTS products. Note that it may be possible for some legacy/COTS products to act as an MSaaS by encapsulating it in a wrapper.
- In current distributed M&S applications, often significant tailoring of gateways etc. is required before use.
- Validation of specific services may be more difficult when they are more remote and internal operation is shielded to a large degree.

- Unwillingness of nations/companies to share resources.
- Unwillingness of companies to move to a pay-per-use model.
- Commercial constraints (e.g., procurement agencies don't like pay-per-use model due to acquisition process constraints and limitations).
- Vendor (cloud provider) lock-in.

2.9 CURRENTLY EXCLUDED

The following aspects are considered to be currently out of scope of the MSaaS concept:

- Internal design of services, development methodology, development tools, etc.

Chapter 3 – IMPLEMENTATION STRATEGY, OPEN TOPICS AND PROPOSED ROADMAP

3.1 IMPLEMENTATION STRATEGY

An incremental development and implementation strategy is proposed for the Allied Framework for M&S as a Service. The incremental approach facilitates a smooth transition in the adoption of an Allied Framework for M&S as a Service and describes a route that will incrementally build an Allied Framework for M&S as a Service.

The proposed strategy also provides a method to control the rate of expansion of the new framework permitting the iterative development and training of processes and procedures. Finally, it permits those nations that have been early adopters of an Allied Framework for M&S as a Service and have national capabilities to accrue additional benefits from their investments and highlight the benefits as well as providing lessons learned and advice to those nations considering similar investments.

As illustrated in Figure 3-1, the MSaaS implementation strategy is broken down into three phases: "Initial Concept Development"; "Specification and Validation"; and "Implementation."

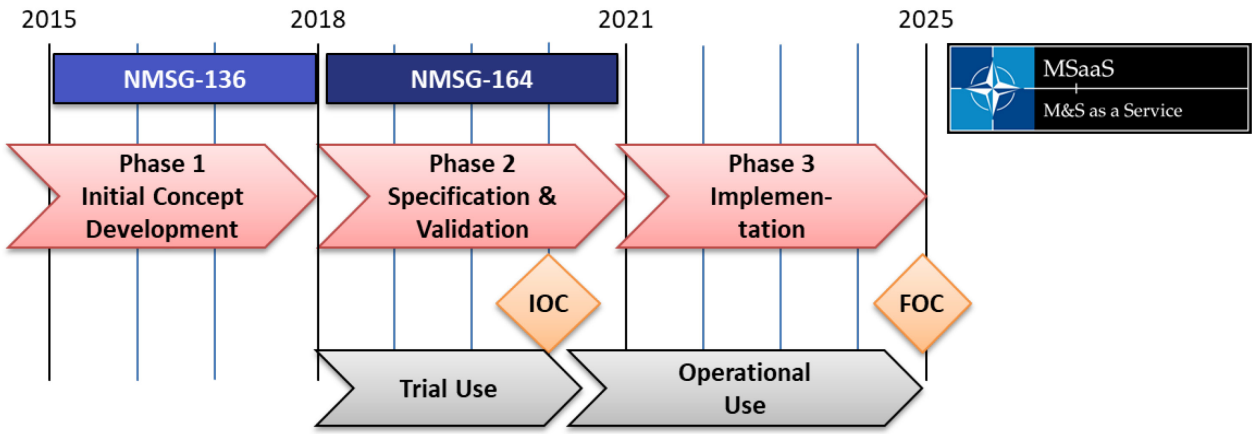

Figure 3-1: MSaaS Implementation Strategy.

1) Phase 1: Initial Concept Development

   The Initial Concept Development (2015 until end of 2017) is executed by NMSG-136 and consists of concept development and initial experimentation. For this period an MSaaS Portal will be provided by individual members of MSG-136 for trial use.

2) Phase 2: Specification and Validation:

   From 2018 – 2021 the initial concepts are extended by NMSG-164 (i.e., specification of issues and challenges not yet addressed) and validated through regular exercise participation and dedicated evaluation events. This phase includes transformation of governance policies into STANAGs or STANRECs, and moving from prototype implementation to operationally usable and mature systems.

   By 2020 Initial Operational Capability (IOC) is established, being defined as an MSaaS solution that is available to an initial set of users. Specifically, IOC will be demonstrated 2020 as part of Trident Jupiter 2020 and 2021 as part of Viking 21.

3) Phase 3: Implementation

By 2025 Full Operational Capability (FOC) is achieved which includes adaptation of many existing simulation related services to the MSaaS Reference Architecture. This is achieved primarily by adding services to the Allied Framework for M&S as a Service.

FOC requires that a permanent MSaaS solution (infrastructure, organization, etc.) is established and that it is available to all interested users.

3.2 OPEN (RESEARCH) TOPICS

The following topics have not yet been addressed and need to be addressed in Phases 2 and 3:

- MSaaS-specific cyber security issues;
- Integration of MSaaS and C2 systems;
- Investigation of MSaaS impacts to Doctrine and Policy;
- Graphical preview of services, i.e., visualization of services as part of the Service Specification to help users understand what a service does (or does not);
- Interface specifications, data format specifications, etc.;
- Integration of national/international registries/repositories and supporting metadata standards;
- Intelligent discovery services, i.e., Amazon/Google-like functionality (“recent studies used this model”);
- Cloud Security: Cross Domain Security in the Cloud, encrypted containers, export control;
- Service oriented architectures/frameworks;
- Semi-automated simulation composition: composition aide, MSaaS design patterns;
- Semi-automated simulation deployment definition;
- Discovery and Composition linked to Event Objectives/Requirements;
- Elasticity: supporting frameworks, load balancing, scalability to millions of entities;
- MSaaS service development: i.e., Information Warfare simulation service, behaviour modelling service, etc.;
- Automated V&V; and
- Procurement approaches.

3.3 ROADMAP

Figure 3-2 shows a roadmap how the topics identified above may be addressed. The capability drivers (top lane) show the potential exploitation path towards realizing the MSaaS vision. The bottom lanes show the required Science and Technology (S&T) activities.

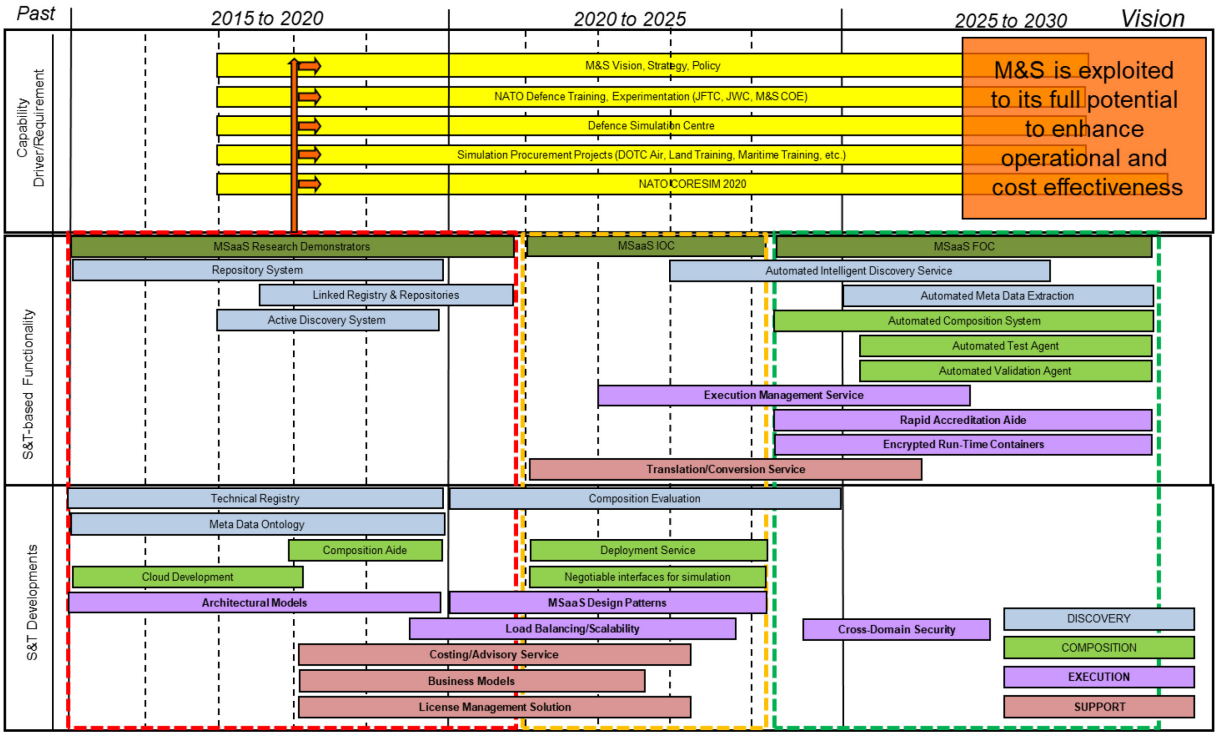

Figure 3-2: MSaaS Roadmap.

Chapter 4 – NON-TECHNICAL ASPECTS

Non-technical aspects (like legal issues, contract/procurement issues, policy issues, etc.) are important for maturing MSaaS. Initial discussion of non-technical aspects is provided in Chapter 5, with a more detailed analysis of the non-technical aspects to be executed in Phases 2 and 3.

Chapter 5 – ANALYSIS OF THE ALLIED FRAMEWORK FOR MSAAS

This chapter provides an analysis of the proposed Allied Framework for M&S as a Service.

5.1 DOTLMPFI IMPLICATIONS OF MSAAS

In the NATO context a capability can be defined as "the ability to execute a specified course of action or achieve a certain effect" and when a new capability is introduced several aspects should be taken into account, adopting the so called "comprehensive approach". Existing components may need changes or new components may need to be developed. The components that have to be considered are: Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability (DOTMLPFI).

In the following, the Allied Framework for M&S as a Service as defined by this OCD is analyzed using the DOTMLPFI approach.

- Doctrine:
  - MSaaS is considered a modernization of existing M&S capability and technology. Although major doctrine changes are not expected, minor revisions or adaptations may be required.
- Organization and Policy (*How to organize NATO and Allied M&S structures*):
  - The need for an Allied Framework for M&S as a Service results from national policies like United Kingdom's Defence Information and Communications Technology Strategy [7], United States Department of Defense (DoD) Cloud Computing Policy [8], the Italian Ministry of Defence (MoD) NEC001 [9] and NATO policies [10].
  - Establishing the Allied Framework for M&S as a Service requires installation of an MSaaS Governance Authority (as defined by AMSP-02 / STANREC 4794) and accompanying policies (e.g., an ETEE policy mandating the sharing of M&S resources). This body will also govern the RA.
  - Establishment of national and NATO "Simulation Centers" that have oversight of MSaaS activities (cp. Governance Authority from previous bullet point).
  - Adopting the Allied Framework for M&S as a Service will influence procurement as M&S services may be acquired on a pay-per-use or share-principle and ownership is not necessarily transferred. This has impacts on the relationship of provider (e.g., industry) and buying authorities.
  - The changes in procurement (see previous bullet) require development and adoption of appropriate Service Level Agreements (SLAs).
  - Sharing of M&S services between NATO and nations (see also below under "Interoperability") may require development and adoption of appropriate Memorandums Of Understanding (MOUs).
- Training (*How to prepare NATO and national MSaaS specialists*):
  - Training is required to prepare users (e.g., Exercise Control (EXCON) and Simulation Control (SIMCON) staff) to fully utilize the Allied Framework for M&S as a Service (e.g., to discover simulation services, to compose and execute services, etc.).
  - MSaaS will require new skills (e.g., regarding cloud computing, virtualization, service-oriented architectures, and emerging M&S-related technology, etc.) and appropriate education and training.

    - MSaaS should enable and transform training in NATO, improving quality and quantity (see Ref. [3]).

- Leadership (*Chain of Command and Control and relationships in NATO and nations according to MSaaS*):
    - To realize the full potential of MSaaS an enterprise approach is required where senior leaders approve the MSaaS concept and support the transformation activities.
- Materiels (*All the hardware, software, equipment and systems related to MSaaS necessary to NATO and nations to manage, to support and to develop M&S Services*):
    - The MSaaS concept requires establishment of a cloud infrastructure and appropriate infrastructure (e.g., network connections).
    - Full adoption of MSaaS requires gradual transformation of existing M&S applications, data, etc. to comply with the MSaaS concept.
- Personnel (*Availability of qualified people according to MSaaS needs*):
    - It is expected that the amount of resources required for preparing and conducting exercises and experimentations are reduced (less personnel to run EXCON/SIMCON, less administration efforts due to automation, etc.).
    - It will likely be required to educate or re-skill personnel to ensure the required amount of Suitably Qualified and Experienced Personnel (SQEP).
- Facilities (*Data Centers, Training facilities and Battle Labs available to provide and to consume MSaaS services*):
    - Cloud infrastructure and appropriate data centers are required.
    - Training facilities (e.g., simulator centers, classrooms) need to be equipped with appropriate infrastructure and need to be connected to simulation networks.
- Interoperability (*How to provide interoperable and accessible MSaaS services in NATO and nations*):
    - The MSaaS concept promotes an open systems approach and strongly favors the adoption of open standards (for data formats, protocols, etc.). If required, existing proprietary solutions need to be replaced by open standards.
    - To enable the MSaaS concept, sharing of M&S resources needs to be mandated.
    - Exchange of classified information (either, single-level or multi-level security) may require adaptation of security policies and alignment between NATO and nations.

5.2 COST-BENEFIT ANALYIS

In order to achieve the full benefits of MSaaS, an ecosystem needs to be established that enables national government and supplier organizations to interact within the MSaaS paradigm. Interoperability of national MSaaS approaches with NATO and allies is essential to realize the full cost and operational benefits achieved through re-use and sharing of simulation resources.

Suitable upfront investment will be required from NATO and nations to operationalize the MSaaS capability (i.e., provision of cloud computing infrastructure, development of MSaaS Portal, provision of facilities and staff to provide coherence and delivery of services). The upfront costs mean that MSaaS would probably not be a cost effective solution if just applied to one particular acquisition project, as it needs to scale across

multiple (preferably all) NATO and national M&S applications. It is thought that scaling across particular M&S communities (i.e., Training, Test and Evaluation, Experimentation) would also be sufficient to provide cost efficiencies. Further studies are required to understand the level of scale of implementation required in order to achieve the benefits required, and how incremental development of MSaaS capabilities can deliver incremental cost and operational benefits so that a "big bang" approach doesn't have to be taken. This will help to provide justification for the MSaaS approach to decision makers and for specific business cases.

Many of the major barriers to fully realizing the benefits of MSaaS are not technical; instead they are related to cultures and behaviors within the ecosystem. While these aren't specifically related to the MSaaS reference architecture, they do represent risks to successful implementation. Key aspects include:

- Suitably Qualified and Experienced Personnel (SQEP): Users of MSaaS capabilities will need to be able to access and utilize the MSaaS Portal and supporting tools. The concept of MSaaS is to ensure a low barrier to entry and provide tools which reduce the training and operational burden.
- Portfolio Management and Coherence: Stovepiped budgets continue to act as a barrier to defence organizations investing in reusability. Coherence through NATO and national simulation strategy and policy is essential for ensuring MSaaS is promulgated within simulation projects across defence.
- Trends in M&S Consumption and Business Models: The way that Defence acquires M&S may need to evolve to fully deliver cost efficiencies that enable both supplier and demander to sustain a sufficient capability. Models such as "Pay per Use" or "Gainshare" for provision of both hardware and software services need to be assessed vs the traditional licensing model.
- Establishing the MSaaS market place: The MSaaS registry of services will need to be seeded over time. Communicating the market place and MSaaS approach to suppliers and demanders so they can suitably inform technology development roadmaps to deliver in line with MSaaS will be key to maximizing the effect.

Initial efforts have been started to execute more detailed and robust cost-benefit evaluations of MSaaS. At the time this document was prepared, results have not yet been available. It is strongly recommended that the follow-on activity (MSG-164, see Chapter 3, Section 3.1) continues the MSaaS cost-benefit analysis.

Chapter 6 – SERVICE TAXONOMY

This chapter presents a service taxonomy that categorizes the different types of services that comprise the Allied Framework for M&S as a Service (see Table 6-1).

A detailed description of individual services (Architecture Building Blocks) is available in MSaaS Volume 1: Technical Reference Architecture.

Table 6-1: MSaaS Service Taxonomy.

Layer	Architecture Building Blocks	Example(s)
57. Operational Systems Layer	• Communication Services	–
	• Infrastructure Services	• Capability to host systems/services • Monitoring, metering and provisioning of infrastructure
58. Service Components Layer	• Business Support Services	–
	• SOA Platform Services	–
59. Services Layer	• M&S Specific Services	• Model and simulate COI capabilities (e.g., Weapon Effects Service)
	• M&S Composition Services	• Standards and tools for capturing composition-related information, e.g., FEAT
	• M&S Orchestration Services	• Orchestration services coordinate joint execution of other services • Google Kubernetes, Docker Swarm, Apache Mesos
	• M&S Simulation Control Services	• Control simulation execution (e.g., start, stop, pause) • Collect simulation results
60. Business Process Layer	• M&S Battlespace Simulation Services	• Create, read, update and delete scenarios
61. Consumer Layer	• M&S User Applications	• User-facing applications
	• ETEE Applications	–
62. Integration Layer	• M&S Message-Oriented Middleware Services	• Capabilities for an exchange of messages between producing and consuming simulation services • HLA, DIS, DDS?
	• M&S Mediation Services	• Simulation gateways (e.g., DIS-to-HLA) • C2Sim gateways

Layer	Architecture Building Blocks	Example(s)
63. Quality of Service Layer	• M&S Platform SMC Services	• Capabilities to manage and control other services • Monitoring, Metering, Logging
	• M&S Platform CIS Security Services	• Capability to implement and enforce CIS security policies • Identity and Access Management?
64. Information Layer	• M&S Metadata Repository Services	• Capability to store, retrieve metadata • NATO SRL
	• M&S Information Discovery Services	• Capability to discover and retrieve information products
	• M&S Model Repository Services	• Capability to store, retrieve and manage simulation service components
	• M&S Information Registry Services	• Capability to store, retrieve and manage references to authoritative information required for execution of simulation models

Chapter 7 – REFERENCES

[1] NATO STO: Final Report of MSG-131, Modelling and Simulation as a Service: New Concepts and Service Oriented Architectures. STO Technical Report TR-MSG-131, Document AC/323(MSG-131) TP/608. May 2015.

[2] NATO: NATO Modelling and Simulation Master Plan, Version 2.0, Document AC/323/NMSG (2012)-015, 14 September 2012.

[3] NATO: 2015 Gap Analysis Report on Modelling and Simulation in support of Military Training, Ser:NU0604.

[4] NATO STO: Final Report of ET-39 Operational Requirements for Training Interoperability. AC/323/NMSG(2017)-003, 21 February 2017.

[5] NATO: NATO Modelling and Simulation Standards Profile. AMSP-01, Edition (D), Version 1. September 2017.

[6] NATO: AMSP-02 Allied Framework for Modelling & Simulation (MSaaS) Governance Policies. Edition (A), Version 1. To be published.

[7] UK Ministry of Defence, Chief Technology Officer. Defence Information and Communications Technology Strategy. UK, 2013.

[8] Department of Defense, Chief Information Officer, Cloud Computing Strategy. Washington, D.C., USA, July 2012.

[9] Stato Maggiore della Difesa, VI Reparto Sistemi C4I e Trasformazione, 2007. SMD – NEC – 001 Linee di indirizzo di Modelling and Simulation per lo sviluppo dei Sistemi C4ISTAR della Difesa. Rome, Italy. SMD document.

[10] NATO Consultation, Command and Control Board (C3B): NATO Cloud Computing Policy, AC/322-D(2016)0001, 7 January 2016.

Annex A – EXAMPLES OF OPERATIONAL USE CASES

This annex provides examples of operational use cases and illustrates which organizations and stakeholders may be involved. This annex is provided for information only and is neither complete nor does it seek to define responsibilities.

A.1 COLLECTIVE TRAINING: COLLECTION OF INTEL INFORMATION

The training audience requires Intelligence (INTEL) information about a specific area of interest (e.g., troops, movements). The information is provided from different sources. The training audience uses the information in their decision making process (see Table A-1).

Table A-1: Collective Training – Collection of INTEL Information Use Case.

	Customer	Users	Provider	Supplier	Required MSaaS Services
Examples	NCIA	JWC, JFTC	NCIA ("NATO Cloud")	Industry, etc.	Joint Simulation, INTEL Report Service, UAV Full Motion Video STANAG compliant, etc.

A.2 TRAINING ON TEAM LEVEL: FORWARD AIR CONTROLLER (FAC)

The training audience (national FAC and pilot) requires a consistent synthetic natural environment. Tactical communication between FAC and pilot is required (see Table A-2).

Table A-2: Training on Team Level – FAC Use Case.

	Customer	Users	Provider	Supplier	Required Capabilities
Examples	National Procurement Agency	Fighter Simulator, FAC Simulator (e.g., Dome)	National MSaaS Cloud Provider	Industry	Synthetic Environment Service, 3d Models, Air Asset, Weapon Effects Service, Communication Effects Service, Tactical Communication Service, etc.

A.3 TRAINING ON INDIVIDUAL LEVEL: CULTURAL AWARENESS

The training audience (individual soldier) has to be trained in Cultural Awareness. The trainee shall be able to do the training from everywhere using his own mobile device or PC (see Table A-3).

Table A-3: Training on Individual Level – Cultural Awareness Use Case.

	Customer	Users	Provider	Supplier	Required Capabilities
Examples	National Procurement Agency	National soldiers (Private up to LTC), using his own laptop, tablet, or mobile phone. Commanding Officer	National MSaaS Cloud Provider, NATO MSaaS Cloud Provider	E-learning provider of armed forces	Cultural Awareness Training Service

An example workflow how this use case may be supported by the Allied Framework for M&S as a Service is presented in Annex B.

A.4 SUPPORT TO OPERATIONS

This use case encompasses activities conducted to ensure that NATO and Nations decision makers and operational commanders have access to capabilities required to decide on, initiate, sustain, and successfully conclude operations [2] (see Table A-4).

Table A-4: Support to Operations Planning Use Case.

	Customer	User	Provider	Supplier	Required Capabilities
Examples	National Procurement Agency	Staff, OR/M&S Officer, Reachback Cell/Unit	National MSaaS Cloud Provider	Defence S&T Organization, Industry	Synthetic Environment Service, Force Structure Service, Route Planning Service

A.5 CAPABILITY DEVELOPMENT

This use case addresses the preparation for the future to foster continuous improvement of military capabilities in order to enhance the interoperability and effectiveness of NATO and nations [2] (see Table A-5).

Table A-5: Capability Development Use Case.

	Customer	User	Provider	Supplier	Required Capabilities
Examples	MoD, DoD, DnD	Force/ Combat/ Capability Developers, Battle Labs, R&T organizations, etc.	National MSaaS Cloud Provider	Defence S&T Organization, Industry	Scenario Development Services, Force Structure Service, CGF service, Generic Adaptable Behavior Model (e.g. to model fictitious vehicles), Data Farming Services (incl. Execution Control Services), Analysis Services

A.6 MISSION REHEARSAL

This use case pertains to the preparation and rehearsal for a planned mission or course of action to reduce risk and surprise and to improve the knowledge and awareness of situations [2] (see Table A-6).

Table A-6: Mission Rehearsal Use Case.

	Customer	User	Provider	Supplier	Required Capabilities
Examples	National Procurement Agency	Higher level commander, Infantry Platoon	National MSaaS Cloud Provider	Industry, etc.	Synthetic Environment (plus live satellite data), Weapon Effects Service, CGF Service, Route Planning Service, After Action Review Service

A.7 PROCUREMENT/ACQUISITION

This use case pertains to the support of total lifecycle management of assets and systems including design risk reduction, test and evaluation. It facilitates appropriate allocation of resources and optimal management for the NATO and Nations defence procurement to ensure the best value for money and to fulfill its missions [2] (see Table A-7).

Table A-7: Procurement/Acquisition Use Case.

	Customer	**User**	**Provider**	**Supplier**	**Required Capabilities**
Examples	National Procurement Agency	Testing center or proving ground that supports a procurement officer or program / project manager.	National MSaaS Cloud Provider	Defence S&T Organization, Industry	Generic/Historical Data Service

Annex B – EXAMPLE WORKFLOW FOR USE CASE "TRAINING ON INDIVIDUAL LEVEL: CULTURAL AWARENESS"

This annex presents an example workflow how the use case "Training on individual level: Cultural Awareness" (see Annex A, Section A.3) may be supported by the Allied Framework for M&S as a Service:

- Commanding Officer identifies need for Cultural Awareness training of his soldiers.
- Commanding Officer defines training requirements and schedules.
- Commanding Officer logs in into MSaaS Portal of his national MSaaS provider and searches for available "Cultural Awareness Training Services":
  - MSaaS Portal shows 5 available services of different quality (3 services in national MSaaS cloud, 2 services in NATO MSaaS cloud). The available services may include serious games, slides, interactive tutorials, etc.
  - Commanding Officer selects 2 services that satisfy his training requirements:
    - 1 service is cost-free; and
    - 1 service has to be paid per hour; the national procurement agency has a contract in place that allows using this service.
  - Commanding Officer creates new Exercise (name "Second Wave").
  - Commanding Officer defines and documents training objectives in MSaaS Portal (e.g., 2 hours per trainee, 80% of tasks have to be executed successfully by trainees).
  - Commanding Officer configures selected training services (scenarios, tasks, etc.).
  - Commanding Officer structures exercise (introductory video, interactive training, etc.).
  - Commanding Officer assigns individual trainees to the exercise.
- Trainees are automatically informed (e.g., via email) that a new exercise has been created and that they have to complete it until end of next month.
- Trainee signs in into MSaaS Portal and clicks on "Start Exercise *Second Wave*":
  - Trainee may use any device (PC in classroom, laptop at home, tablet, etc.).
  - Trainee completes training with 91% success rate.
- Commanding Officer sees status of all trainees (e.g., exercise started, exercise in progress, exercise completed) and individual evaluation reports.
- Exercise results are added to the individual trainee's personnel file.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-MSG-136-Part-III AC/323(MSG-136)TP/830	ISBN 978-92-837-2156-7	PUBLIC RELEASE

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Operational Concept Document (OCD) for the Allied Framework for M&S as a Service

7. Presented at/Sponsored by

Developed by NATO MSG-136.

8. Author(s)/Editor(s)	9. Date
Multiple	May 2019
10. Author's/Editor's Address	**11. Pages**
Multiple	60

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Cloud computing
Composability
Distributed simulation
Interoperability
Live, Virtual, Constructive (LVC) Modelling
Modelling and Simulation (M&S)
Modelling and Simulation as a Service (MSaaS)
M&S Services
NATO C3 Classification Taxonomy
Reference architecture
Service-Oriented Architecture (SOA)
Simulation
Simulation Architecture
Simulation Environments
Simulation Interoperability

14. Abstract

M&S as a Service (MSaaS) is a concept that combines service orientation and the provision of M&S applications via the as-a-service model of cloud computing to enable more composable simulation environments that can be deployed and executed on-demand. NATO MSG-136 investigated the concept of MSaaS and provided technical and organizational foundations to establish the Allied Framework for M&S as a Service within NATO and partner nations. The Allied Framework for M&S as a Service is the common approach of NATO and nations towards implementing MSaaS and is defined by the Operational Concept Document, Technical Reference Architecture, and MSaaS Governance Policies.

This document describes the Operational Concept for the Allied Framework for MSaaS. The Operational Concept Document (OCD) describes the intended use, key capabilities and desired effects of the Allied Framework for M&S as a Service from a user's perspective.

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DIFFUSION DES PUBLICATIONS
STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALIE
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

ROUMANIE
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 06 Liptovský Mikuláš 6

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

The British Library Document
Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and
Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESTONIA
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALY
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 06 Liptovský Mikuláš 6

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down, Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-92-837-2156-7