NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-164)TP/1185

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-164-Vol-III**

Business Model for the Allied Framework for M&S as a Service

(Modèle économique du cadre allié de M&S en tant que service)

Developed by NATO MSG-164.

Published April 2024

Distribution and Availability on Back Cover

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(MSG-164)TP/1185

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-164-Vol-III**

Business Model for the Allied Framework for M&S as a Service

(Modèle économique du cadre allié de M&S en tant que service)

Developed by NATO MSG-164.

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 April 2024

ISBN 978-92-837-2497-1

Table of Contents

List of Figures

List of Tables

MSG-164 Membership List

CO-CHAIRS

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

Mr. Tom VAN DEN BERG
TNO
NETHERLANDS
Email: tom.vandenberg@tno.nl

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

Mr. Christopher MCGROARTY
US Army CCDC – DEVCOM SC
UNITED STATES
Email: christopher.j.mcgroarty.civ@army.mil

MEMBERS[1]

Mr. Boon-Hwa ANG
Defence Science and Technology Agency (DSTA)
SINGAPORE
Email: aboonhwa@dsta.gov.sg

Dr. Michael BERTSCHIK
Bundeswehr
GERMANY
Email: michaelbertschik@bundeswehr.org

LTC (OF4) Dr. Marco BIAGINI
ITA MoD
ITALY
Email: r5cscgc@sgd.difesa.it

Ms. Martina BINI
Leonardo S.p.A.
ITALY
Email: martina.bini@leonardocompany.com

Dr. Paolo BOCCIARELLI
University of Rome Tor Vergata
ITALY
Email: paolo.bocciarelli@uniroma2.it

Mr. Michiel BON
Dutch MoD
NETHERLANDS
Email: Netherlandsmf.bon@mindef.nl

Mr. Maxwell BRITTON
Department of Defence
AUSTRALIA
Email: alexburne@skymesh.com.au

Mr. Ahmet-Birol CAVDAR
HAVELSAN A.S.
TÜRKIYE
Email: abcavdar@havelsan.com.tr

Dr. Anthony CRAMP
Defence Science and Technology Group of the
Australian Department of Defence
AUSTRALIA
Email: anthony.cramp@defence.gov.au

Prof. Andrea D'AMBROGIO
University of Roma TorVergata
ITALY
Email: dambro@uniroma2.it

Mr. Marius DICKEBOHM
German Armed Forces
GERMANY
Email: Marius1Dickebohm@bundeswehr.org

Dr. Salvatore D'ONOFRIO
Leonardo S.p.A
ITALY
Email: salvatore.donofrio@leonardocompany.com

[1] MSG-164 attracted a large number of members. While some of them formed the core group and participated over the whole lifecycle of MSG-164, many subject matter experts and representatives of various communities of interest participated in specific meetings only. The membership list includes all members who participated in at least one meeting or contributed significantly to MSG-164 deliverables.

Mr. Efthimios DOUKLIAS
Joint Staff J6, Joint All-Domain Command and Control (JADC2)
UNITED STATES
Email: efthimios.d.douklias.civ@mail.mil

Ms. Katherine ESCOBAR
Joint Staff J6
UNITED STATES
Email: katherine.b.escobar.civ@mail.mil

Dr. Christian FAILLACE
Leonardo S.p.A
ITALY
Email: christian.faillace@leonardocompany.com

Mr. John FERRELL
Lockheed Martin
UNITED STATES
Email: john.ferrell@lmco.com

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

Mr. Brad FRIEDMAN
Army Futures Command
UNITED STATES
Email: brad.d.friedman.civ@army.mil

Mr. Scott GALLANT
Effective Applications Corporation
UNITED STATES
Email: scott@EffectiveApplications.com

Mr. Sabas GONZALEZ GODOY
NATO ACT
ACT – ALLIED COMMAND TRANSFORMATION
Email: Sabas.Gonzalez@act.nato.int

Mr. Yannick GUILLEMER
French Ministry of Armed Forces
FRANCE
Email: yannick.guillemer@intradef.gouv.fr

Mr. Douglas HENRY
Dstl
UNITED KINGDOM
Email: djhenry@dstl.gov.uk

Dr. Andre HOOGSTRATE
Ministry of Defense
NETHERLANDS
Email: aj.hoogstrate@mindef.nl

Mr. Tom HOUWELING
Defence Material Organisation (DMO)
NETHERLANDS
Email: tlj.houweling@mindef.nl

Mr. Willem HUISKAMP
TNO Defence Research
NETHERLANDS
Email: wim.huiskamp@tno.nl

Mr. John HUTT
US Air Force Agency for Modeling & Simulation (AFAMS)
UNITED STATES
Email: john.hutt@us.af.mil

Mr. Lars JANSSON
Swedish Defence Material Administration (FMV)
SWEDEN
Email: lars.jansson@fmv.se

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

Mr. James KEARSE
NSC Ltd
UNITED KINGDOM
Email: james.kearse@nsc.co.uk

Mr. Rob KEWLEY
simlytics.cloud LLC
UNITED STATES
Email: rob@simlytics.cloud

Mr. Gerardus KONIJN
Ministry of Defence
NETHERLANDS
Email: GA.Konijn@Mindef.nl

Mr. Niels KRARUP-HANSEN
MoD DALO
DENMARK
Email: niels@krarup-hansen.dk

Mr. Patrice LE LEYDOUR
Thales
NIAG-NATO INDUSTRIAL ADVISORY GROUP
Email: patrice.leleydour@thalesgroup.com

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

Mr. Björn LÖFSTRAND
Pitch Technologies AB
SWEDEN
Email: bjorn.lofstrand@pitchtechnologies.com

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

Dr. Giovanni MAGLIONE
NATO STO CENTRE FOR MARITIME RESEARCH AND EXPERIMENTATION
CMRE
Email: Giovanni.Maglione@cmre.nato.int

Mr. Benjamin MAGUIRE
Defence Science and Technology Group of the Australian Department of Defence
AUSTRALIA
Email: ben.maguire@defence.gov.au

Mr. Hans MULDER
Antwerp Management School
NETHERLANDS
Email: Hans.Mulder@ams.ac.be

Mr. Agatino MURSIA
Leonardo S.p.A
ITALY
Email: agatino.mursia@leonardo.com

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

Mr. Dirk OUDE EGBRINK
Royal Netherlands Aerospace Center NLR
NETHERLANDS
Email: dirk.oude.egbrink@nlr.nl

Mr. Bharatkumar PATEL
Dstl
UNITED KINGDOM
Email: bmpatel@dstl.gov.uk

Mr. Dominique PALABOST
CASPOA – NATO Air Operations Centre of Excellence
COE – Air Operations (CASPOA)
Email: dominique.palabost@intradef.gouv.fr

Mr. Robbie PHILLIPS
Lockheed Martin
UNITED STATES
Email: robbie.phillips@lmco.com

Mr. Marco PICOLLO
Leonardo S.p.A
ITALY
Email: marco.picollo@leonardocompany.com

Mr. Johnny POWERS
Lockheed Martin
UNITED STATES
Email: johnny.j.powers@lmco.com

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

Dr. Manfred ROZA
NLR – National Aerospace Laboratory
NETHERLANDS
Email: Manfred.Roza@nlr.nl

Mr. José RUIZ
DGA
FRANCE
Email: jose.ruiz@intradef.gouv.fr

Mr. Angel SAN JOSE MARTIN
ACT
ACT – ALLIED COMMAND TRANSFORMATION
Email: Angel.SanJoseMartin@act.nato.int

LTC (ret) Wolfhard SCHMIDT
ST Engineering Antycip SAS
UNITED KINGDOM
Email: Wolfhard.schmidt@steantycip.com

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

Mr. Chris STRUSELIS
ST Engineering Antycip
UNITED KINGDOM
Email: chris.struselis@steantycip.com

MAJ Rafal SUPLATOWICZ
NATO JFTC
JFTC – JOINT FORCES TRAINING CENTRE
Email: rafal.suplatowicz@jftc.nato.int

Mr. Chong-Lai TEO
Defence Science & Technology Agency
SINGAPORE
Email: tchongla@dsta.gov.sg

LTC Davide-Marco TRIMANI
Modelling and Simulation Centre of Excellence
COE – MODELLING AND SIMULATION (MS)
Email: mscoe.cde08@smd.difesa.it

Capt Pascal TRUCHON
Canadian Armed Forces
CANADA
Email: Pascal.Truchon@gmail.com

Mr. Andrew WARHURST
Department of Defence
AUSTRALIA
Email: Andrew.Warhurst2@dst.defence.gov.au

Business Model for the Allied Framework for M&S as a Service

(STO-TR-MSG-164-Vol-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-164 ("Modelling and Simulation as a Service – Phase 2") developed 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:

- Allied Framework for M&S as a Service (MSaaS), Operational Concept Document (STO-TR-MSG-136-Part-III);
- Allied Framework for M&S as a Service (MSaaS), Concept of Employment (AMSP-02);
- Business Model for the Allied Framework for M&S as a Service (MSaaS) (STO-TR-MSG-164-Vol-III);
- Modelling and Simulation as a Service (MSaaS) Technical Reference Architecture ((STO-TR-MSG-164-Vol-II).

This document discusses the concept of an MSaaS ecosystem from a business model perspective and is part of the blueprint towards this capability.

Modèle économique du cadre allié de M&S en tant que service

(STO-TR-MSG-164-Vol-III)

Synthèse

L'OTAN et les pays utilisent les environnements de simulation à différentes fins, telles que la formation, le développement des capacités, la répétition des missions 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. Les produits de M&S sont des ressources extrêmement précieuses ; il est essentiel que les produits, données et procédés de M&S soient commodément accessibles à un grand nombre d'utilisateurs aussi fréquemment que possible. Toutefois, l'interopérabilité entre 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 de la 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-164 de l'OTAN (« Modélisation et simulation en tant que service – Phase 2 ») a développé 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 suivants :

- Cadre allié de M&S en tant que service (MSaaS), document de définition opérationnelle (OCD) (STO-TR-MSG-136-Part-III) ;
- Cadre allié de M&S en tant que service (MSaaS), concept d'emploi (AMSP-02) ;
- Modèle économique du cadre allié de M&S en tant que service (MSaaS) (STO-TR-MSG-164-Vol-III);
- Architecture de référence technique de la modélisation et simulation en tant que service (MSaaS). ((STO-TR-MSG-164-Vol-II) ;

Le présent document aborde le concept d'un écosystème de MSaaS dans l'optique d'un modèle économique et fait partie du plan détaillé pour établir cette capacité.

BUSINESS MODEL FOR THE ALLIED FRAMEWORK FOR M&S AS A SERVICE

1.0 INTRODUCTION

1.1 Background and Key Drivers

Modelling and Simulation (M&S) is a key enabler for the delivery of capabilities to NATO and Nations in the domains of training, analysis and decision making. M&S solutions need to be integrated seamlessly in future information system capabilities to ensure increased responsiveness, efficiency, affordability, interoperability, and reusability. This strategic objective is formally captured in the NATO Modelling and Simulation Vision in the NATO M&S Masterplan [1].

The need to be more responsive is driven by an increasingly complex, competitive, and connected world that defines the future threats and hybrid environments that NATO defence forces will operate in. The challenge for the Allied forces is not so much in responding to what we know today, but to be fully prepared for what tomorrow might bring.

The NATO Strategic Foresight Analysis 2017 [2] provides a wide-ranging shared understanding of the future security environment. It describes the future NATO expects towards 2035 and beyond. The SFA depicts the future in terms of political, human, technological, economic, and environmental trends. Where trends may move in diverging directions, SFA provides an alternative view to maintain objectivity. The SFA is currently being updated to SFA 2021.

A key finding is that the future M&S needs will be much broader, characterized by not only traditional warfare domains (Air, Land, Sea), but including new domains (Space, Cyber and Electronic) that impact the security of NATO and Nations.[1] M&S capabilities will need to represent an operating environment that is hybrid in nature, rapidly evolving, and with a wide spectrum of threats and effects to security. Many of today's M&S capabilities are too focused on traditional warfare and developed through traditional procurement cycles that are unlikely to meet the future needs of operational users.

Such an increase in M&S requirements must consider affordability, sustainability, and maintainability as defence budgets are unlikely to increase or even be prioritized towards M&S capabilities. Increasing the efficiency and reusability of M&S capabilities across NATO and its nations is key to making M&S more affordable, and ultimately to achieve the vision of M&S being fully integrated into all operations. There will be the need within the NATO coalition and also within the national M&S communities for greater sharing of models and simulations to leverage investments and encourage greater interoperability to be able to execute the right simulations whenever needed.

> The "Allied Framework for M&S as a Service" or MSaaS ecosystem in the NATO coalition will be based on a federated approach of national and NATO services and service providers that is enabled by a common technical reference architecture, common processes and a common business model (Figure 1).

[1] https://www.nato.int/cps/en/natohq/topics_175419.htm

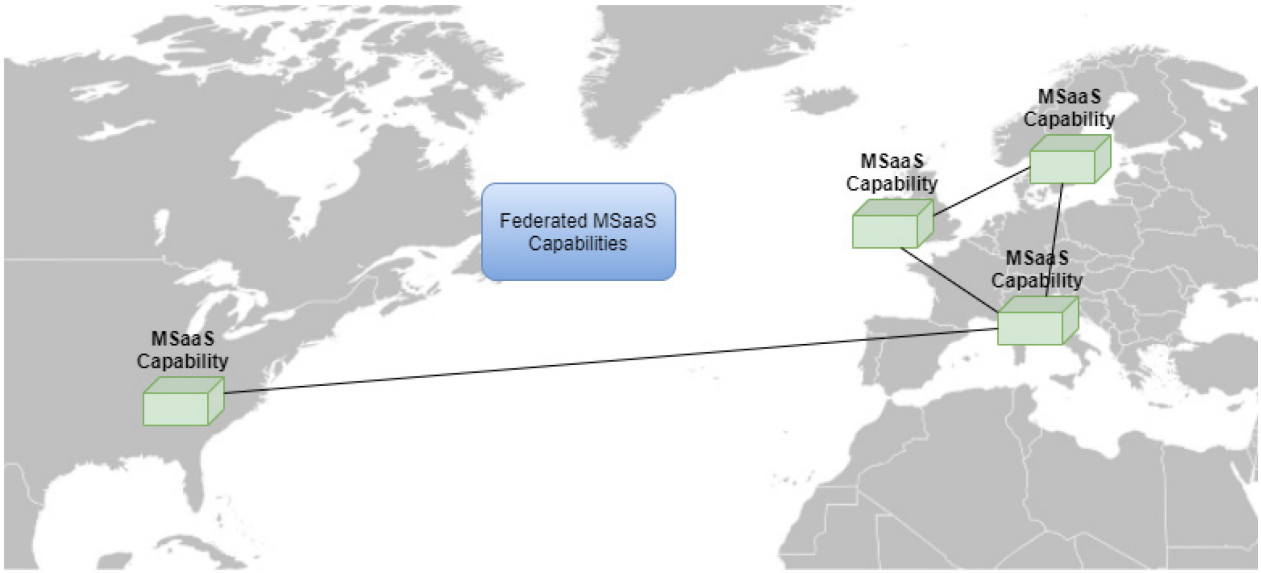

Figure 1: Notional MSaaS Ecosystem Consisting of Federated National and NATO MSaaS Ecosystems.

The application of a "services" model to Modelling and Simulation became known as "Modelling and Simulation as a Service" (MSaaS) and has the potential to greatly reduce the barriers of cost and accessibility and to result in greater utility of M&S throughout NATO and the Nations. The motivation behind MSaaS originated from developments in the area of Service Oriented Architectures (SOA) – mainly in the commercial software development sector. More recently the motivation for MSaaS has been aligned to modernizing defence through adopting commercial practices (e.g., ecosystems, online on-demand services at point of need) and exploiting commercial technologies (e.g., cloud computing, virtual reality, smartphones).

The NATO Modelling and Simulation Group (NMSG) considers MSaaS to offer great opportunities for providing M&S capabilities that address the above shortfalls and initiated several task groups to investigate and demonstrate this technology.

This document discusses the concept of an MSaaS ecosystem from a business model perspective and is part of the blueprint towards this capability (see Section 1.3).

1.2 Characterizing the Future

The MSaaS concept is designed to address a number of challenges as highlighted in the NATO Strategic Foresight Analysis (SFA), summarized below.

The political trends are characterized by:

- Fundamental changes in the international security environment;
- Power transitions from West to East;
- Power diffusions from governments to non-state actors worldwide;
- Increasing instability within the post-Cold War world order; and
- Greater public discontent and increasing challenges to governance.

The Human trends are defined by:

- Asymmetric demographic change, within the developed world an ageing population requiring more priority over defence budgets, and in developing nations' youth unemployment and unrest;
- Rapid urbanization (Megacities, Littoral areas), giving rise to resource scarcity and challenges to distribution of available resources;
- Increasingly fractured and polarized societies;
- Interconnected human networks, which brings both opportunities and challenges; and
- Increasingly, loss of authority of elected bodies and experts.

The Economic/Resources trends are characterized by:

- Globalization has opened markets and intensified economic integration, resulting in increasing influence of developing countries and straining natural resources.
- Largest generation wealth transfer will take place in our lifetime.
- Global economic transformation from automated/manual processes to a fully digitized economy.
- Managing agreements will be transformed to account for rapid operational flexibilities and scalability.
- Emerging markets shifting jobs to countries and regions with cheap labor, giving rise to eroding the economic base for the working middle class in Western countries, fueling social inequality.

The Natural Environment trends will be defined by:

- Climate change, with far-reaching and cross-cutting impacts and Increasing incidences of natural disasters;
- Increasing demand for natural resources;
- Water and food security are growing concerns;
- Losses in bio-diversity;
- Stress on the ecosystem services may reduce resilience; and
- The effects of and response to Epidemics and Pandemics.

The Technology trends are important to the NATO S&T Organization and will:

- Shape the social, cultural, and economic fabrics of our societies at all levels;
- Offer enormous opportunities (not just to us, but also to our adversaries), particularly offensive cyber, Artificial Intelligence (AI), autonomous systems, synthetic biology, and human enhancement;
- Bring new vulnerabilities and challenges as the world digitizes;
- Give rise to fake news; and
- Make defence and security overly dependent on civilian technology and infrastructure.

MSaaS will therefore need to be responsive in rapidly representing many of the resulting effects for defence and security M&S applications, whilst at the same time taking advantage of some of the opportunities (e.g., flexibility, resource sharing, connectivity) and addressing risk (e.g., cyber resilience) that these trends bring.

1.3 MSaaS Developments in NMSG

The Allied Framework for MSaaS is the common vision and approach of NATO and Nations towards implementing MSaaS and is defined by the following documents:

- **Operational Concept Description (OCD):** Describes the general vision and concepts of MSaaS, the intended use, key capabilities, and desired effects of the Allied Framework for MSaaS from a User's perspective [3].
- **Business Model:** The Business Model (this document) describes how MSaaS will manage and enable the intended use, key capabilities, and desired effects of the Allied Framework for M&S as a Service from a Stakeholder's perspective in the multi-government business space. It also defines the methods and means to enable MSaaS as demand-supply ecosystem.
- **Technical Reference Architecture:** The Technical Reference Architecture (TRA) describes the architectural principles, patterns, and best practices for realizing MSaaS capabilities. The TRA discusses the Provider and Supplier perspective [4].
- **Concept of Employment:** The MSaaS Concept of Employment is the governance document that identifies MSaaS stakeholders, their relationships, and utilizes the business model and technical architecture to implement and sustain the Allied Framework for M&S as a Service as a persistent capability [5].

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

1.4 Document Structure

This document defines the vision of a Business Model for MSaaS. The Business Model is to deliver the "MSaaS Value Proposition" in accordance with the overarching vision of NATO and the NMSG as stated in the NMSMP [1].

Section 2 introduces the Business Model for MSaaS, Section 3 discusses expected benefits and risks, the final chapters discuss an incremental implementation strategy.

The Appendices provide Terms and Definitions, Examples and a discussion on Identified Stakeholders and their roles and interactions.

2.0 BUSINESS MODEL FOR M&S AS A SERVICE

2.1 Framework

The purpose of the Business Model (BM) for the Allied Framework for M&S as a Service (MSaaS), that was developed based on the Osterwalder and Pigneur's (2010) Business Model Canvas [6]), is to inform relevant stakeholders how the MSaaS ecosystem will operate in the multi-government business space for the sharing of M&S technologies and services. The Business Model Canvas is a strategic management template for developing new or documenting existing business models. It is a visual chart with elements that describe the organization's value proposition, infrastructure, customers, and finances.

It assists organizations in aligning their activities by illustrating potential trade-offs. This section provides the elaboration of the MSaaS Business Model, Figure 2 shows the visual chart. It shows typical defence and security perspectives that are currently being considered for the MSaaS BM.

The Canvas was developed in a number of sessions with members of MSG-164 and invited participants from different stakeholder organizations. The following paragraphs will discuss the Canvas in more detail.

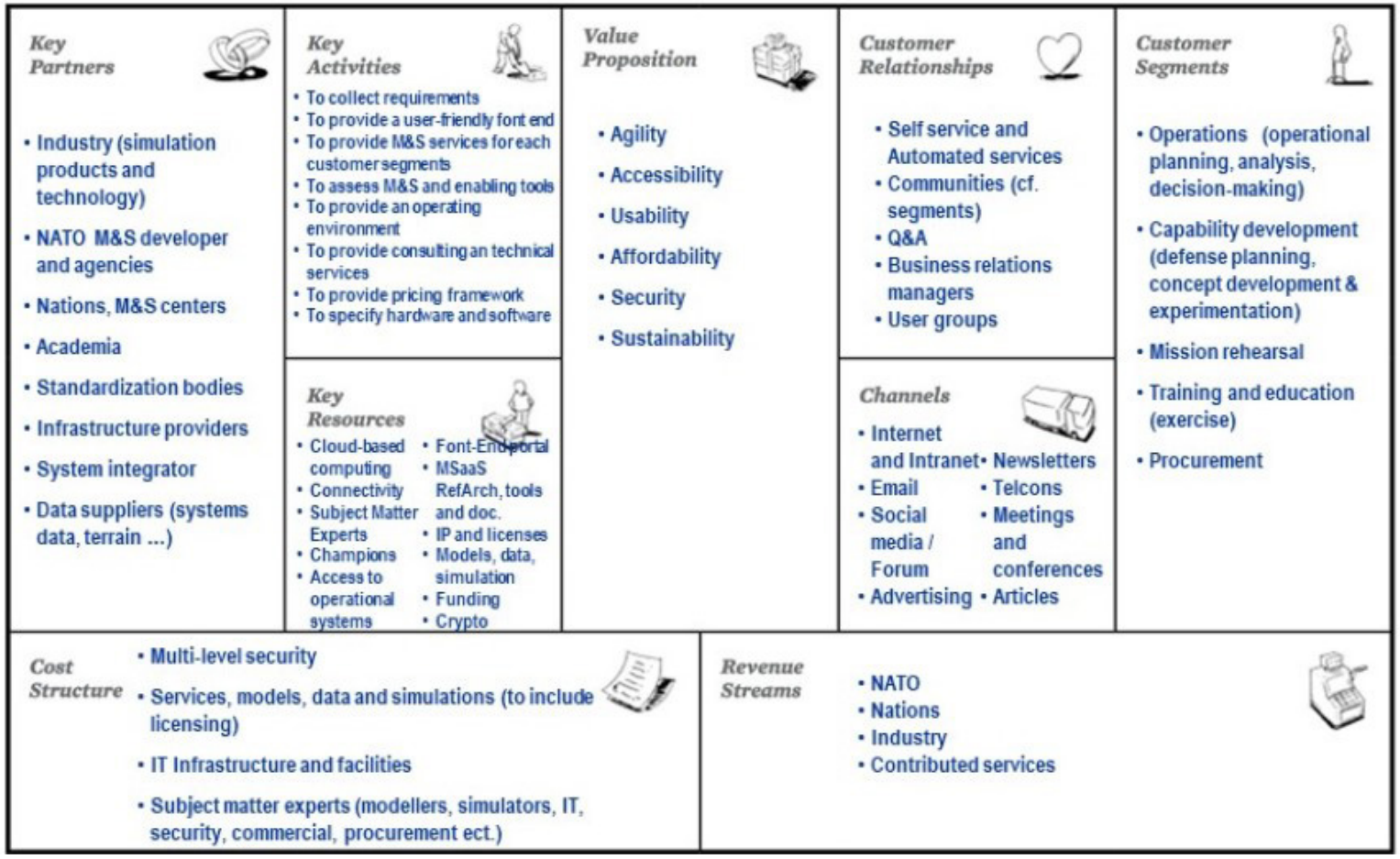

Figure 2: MSaaS Business Model Canvas.

2.2 MSaaS Ecosystem

The MSaaS ecosystem is essentially the marketplace characterized by Customers/Applications (training, mission planning, procurement, etc.), Platform dependent (the Infrastructure as a Service (IaaS) and common Platform as a Service (PaaS) capabilities to support Applications), Niche (Defence, and dual civilian-military) marketplace.

2.3 Stakeholder Segments

Stakeholders can be segmented into distinct groups (roles) based on needs, behaviors, and other traits that they share. The stakeholder segment is defined by their roles as described by the MSaaS Operational Concept Description (OCD) [3] based on their MSaaS Business and operational needs interactions. At the top level, the Stakeholders can be classified as Service Producers and Service Consumers, These two categories can be further divided into respectively, Suppliers / Providers and Customers / Users.

The following paragraphs define the Stakeholders role and their relationships. (See also Appendix 2 for an example showing their interactions.)

2.3.1 Customers

According to the MSaaS definitions [4], the Customers are Defence organizations with an operational need (e.g., training, mission planning, acquisition), and are the budget holder.

The Customer will assist the User by capturing the capability needs based on the operational needs and breaking these down in technical requirements. The requirements will be submitted to potential Suppliers with a request to propose service-based solutions.

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 SLA must be tailored according to specific technical requirements (e.g., functionality, performance), availability requirements (e.g., Demo, Exercise, or persistent Training Capability) and business conditions (e.g., liability, metering, and cost). Different Providers will offer different service solutions and implementations. Customer will assess the offers and decide on a Provider or Supplier. A sample SLA Template (SLAT) can be found in the MSaaS Concept of Employment [5]. The template may serve as guideline. The SLA may be considered a ‘Gentlemen’s Agreement’ regarding “Best Effort” in case of a Demo or Experiment. In case of a commercial service, it obviously needs to be considered as a “Contract” agreed on by the Stakeholders and formally approved by legal and commercial departments.

The SLA Template (SLAT) should be maintained as well by capturing lessons learned collected during its use and improving/supplementing it in consultation with the stakeholders.

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.

2.3.2 Providers

Service Providers will engage with Suppliers to acquire and integrate M&S products and services 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.

2.3.3 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 provide feedback to 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.

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 two User sub-categories Simulation Users and Operational users.

2.3.4 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.

2.4 Key Partners

The Key partners for MSaaS Business Model implementation include:

- Industry (Simulation products and technology);
- NATO M&S developers, NATO M&S agencies (e.g., NCIA);
- Nations, M&S centers;
- Procurement Agencies (e.g., nations, NSPA);
- Academia;
- Standardization Bodies (NATO and International);
- Accreditation Bodies (NATO and International);
- Infrastructure providers (internal and external, data centers/clouds, networks, etc.);
- System integrators; and
- Data suppliers (systems or equipment data, terrain, weather, INTEL, etc.)

Note that the partners mentioned above may have multiple roles: Industry may be Suppliers in some cases but could also be Customers for specific services in other cases (Business to Business (B2B)).

2.5 Key Activities

Key activities are considered relevant in order to satisfy the value propositions. The activities will be performed by one or more Stakeholders.

- Continuous collection of customer and/or user requirements;
- Provide a User-friendly front-end including secure access (e.g., Portal, see Refs. [4], [7], [8]);
- Provide managed services for each customer segment (applications);

- Continuous assessment of models, simulation and enabling tools;
- Provide an operating environment [4];
- Define interoperability requirements [4];
- Provide consulting and technical services;
- Provide pricing framework; and
- Specify hardware, software, and communication requirements [4].

2.6 Key Resources

The following Key Resources will be required to deliver the MSaaS Value proposition:

- Cloud-based computing (public, private or hybrid clouds);
- Connectivity;
- Subject matter experts (modellers, simulators, IT, security, commercial, procurement, etc.);
- Champions: Senior stakeholders, day to day personnel;
- Access to operational systems (e.g., C2-systems, flight simulators, etc.);
- Front-end (Portal);
- MSaaS operating environment (e.g., virtualization software, container software, etc.), tools and documentation;
- Intellectual Property Rights (IPR) and License agreements;
- Models, data, and Simulations; and
- Crypto, Cross Domain Security (hardware and/or software and policies).

2.7 Value Proposition

The MSaaS Value proposition is stated as follows:

> *Agile and user-friendly services that are readily accessible to compose and execute the required modelling and simulation environment that is sustainable, affordable, scalable, and secure.*

To deliver MSaaS to the Stakeholders, the values needed are further specified and detailed:

- Agility in terms of: adaptability, flexibility, scalability, reusability, rapid delivery, speed, tailorable/configurable, operational effectiveness, stay current with emerging technology.
- Accessibility in terms of: availability, user-friendly, maintainability, reliability, performance, online/on-demand, multi-users.
- Usability in terms of: intuitive, user-friendly, easy to compose and execute.
- Affordability in terms of: cost effective, risk reduction, shareable, cost reduction, prevent stovepipes, operational efficiency.
- Security in terms of: classified, unclassified, commercial, accredited, credentials.
- Sustainability: maintain expected level of services.

MSaaS: is thus enabling all stakeholders to address the following current challenges:

- Interoperability between systems, services, and data: addressed through a common agreed MSaaS Reference Architecture that enables service composition;
- M&S support resourcing: improved quality and support through discoverability of shared and pooled M&S assets, services, and expertise;
- Budgetary constraints: addressed through improved sharing and pooling of M&S assets, services, and expertise;
- Validation and accuracy constraints: provision of common services to ensure a common synthetic environment for fair-fight.

2.8 Customer Relationships

The following Customer Relationships have been identified:

- Self-service and Automated services (through MSaaS Portal);
- Communities active in the same segment/application domain;
- Q&A with Subject Matter Experts (SMEs) (e.g., Forum on the MSaaS Portal);
- Business Relations Manager; and
- User Groups (e.g., Forum on the MSaaS Portal, F2F meetings at Conferences).

The MSaaS Portal will be an important access point enabling Customers to communicate and engage with other Stakeholders and communities.

2.9 Stakeholders Channels

While various channels of communication will be available, the highly encouraged means to communicate within the MSaaS ecosystem will be through the MSaaS Portal (Glossary) [4]. Main communication channels include:

- Emails, Newsletters (on MSaaS Portal);
- Video or Telcons (e.g., Webex, Skype);
- Social Media;
- Meetings and Conferences (e.g., NMSG Symposia);
- Forums (on MSaaS Portal);
- Formal Documentation on MSaaS (e.g., MSaaS Reference Architecture);
- Papers and Articles;
- Lecture Series; and
- Advertising and Tradeshows.

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 [3], [4].

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 the 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 [4] are:

- Discover;
- Compose;
- Deploy; and
- Execute.

2.10 Customer Segments

The Customer Segments and their Operational needs are recognized in accordance with the NATO M&S Masterplan (NMSMP) Application Areas [1]:

- Operations (Operational Planning, Analysis, Decision Making);
- Capability Development (Defence Planning, Concept Development and Experimentation);
- Mission Rehearsal;
- Training and Education (Exercises); and
- Procurement.

The different application areas will all be able to benefit from the MSaaS proposition. Specific needs or constraints may be different or stricter (e.g., security requirements for mission rehearsal) depending on the domain.

2.11 Cost Structure

There is an inherent cost to doing business when adhering to the MSaaS construct. Key cost drivers include:

- **Cost to maintain an Open architecture** – Enables free movement of components from one platform to another. Open architecture means selection of technologies that exist as projects contributed to and maintained via open software standards (Linux, Apache, etc.). Adherence to these standards as specified in the MSaaS Technical Reference Architecture [4] prevents vendor lock-in and the ability to disrupt and put NATO components at the forefront of technology.
- **Cost to adhere to standard communications protocols** – Core technologies will need to communicate at speed and at scale. This requires that the services and components support interoperability through recommended NATO M&S interoperability standards [9].
- **Cost to Maintain Continuous Security Accreditation** – Where appropriate, technologies should be certified and adhere to the security standards as set forth by the Accreditation Authorities responsible for the security of the data and communications of the component. Furthermore, considerations for multi-level security and Cross Domain environments should be in place to support NATO simulation events when required [7].
- **Cost of ensuring compatibility with off-line / on-premises implementations (at the edge)** – While many MSaaS instances may involve online implementations (cloud, distributed simulation, etc.), MSaaS providers should work with supplier to ensure that technologies run transparently without broader interconnections with the NATO MSaaS in order to service use cases where connectivity is limited. Any on-premises installation should adhere to the above criteria and be able to be migrated to another platform without refactoring or re-engineering.

- **Cost of services, models, data, and simulations (to include licensing) –** The diversity in the current military simulation space demonstrates a mix of government-owned, government-leased and third party software applications. In turn, MSaaS will likely result in a similar mix in its ecosystem where piece parts or full software applications can be purchased for a limited time or in perpetuity. It is to be expected that the use of MSaaS inherently will have a cost to access elements of the ecosystem. Similarly, certain models and data that support the simulation environments may have additional cost. Examples could include high fidelity systems models or complex terrain environments.
- **Cost of IT Infrastructure and facilities –** Whether an organization chooses to own their own infrastructure or purchase remote infrastructure (e.g., cloud), there is an inherent cost to hardware and software, including maintenance, modernization, and the bandwidth to access remote infrastructure. Remote infrastructure has additional costs based on storage, access, and security. It should be noted that simulation is not always analogous to other software applications and may require additional remote capability that a typical IT department may not consider when they plan for costs. Note that the above does not consider costs for simulation specific hardware that are not generic IT and that include systems either permanently located at point of need (e.g., mock-ups, displays, domes) or that are perhaps mobile. These costs are not specific to MSaaS and will also incur for classical solutions.
- **Cost of Subject Matter Experts (SME) –** Computing in general, and even more so simulation, requires SMEs who understand the modelling, simulation implementations and interfaces, IT, security, etc. There is additional cost in the process of procurement that requires SMEs in business, contracting and other non-technical fields. Akin to specialized simulation today, there will be a cost to acquire the SME(s) associated with implementing a model or simulation, developing scenarios/vignettes for a simulation, or extending a simulation or service to have additional capability based on a use case.
- **Cost of Local Implementations for Execution –** Organizations across NATO are going to have different management practices for implementing MSaaS. In turn, there may be costs to develop user interfaces to access and manage the local implementation of MSaaS, whether that is truly local only, connecting to remote instances or a hybrid. There may also be user accounts, access controls and other implementation requirements specific to an implementing organization.
- **Cost of Modernization and Maintenance –** Across the above costs, whether it is IT refresh, new security requirements or merely managing the MSaaS ecosystem, there is an expectation that modernization will need to occur in various sectors. MSaaS is not something you simply "install" and have implemented akin to a traditional piece of software. As an ever-evolving environment with associated ecosystem, there will be a cost to modernize the system and like all computing, there will be a maintenance cost that must be planned for.

While there are many costs to be considered when implementing MSaaS within an organization, many of these costs are not unique to MSaaS. The goal of the MSaaS business model is to provide a value-driven approach where best-of-breed services are available on demand (flexible use, sharing and pooling to reduce development and maintenance cost). The approach also aligns better with considering costs for the whole life cycle of a simulation capability. In turn, following the MSaaS model provides opportunities for suppliers to bring new capabilities in response to emerging user needs while also potentially driving down costs.

2.12 Revenue Streams

The MSaaS sources of revenue (includes money and services) are:

- NATO;
- Nations;
- Industry (B2B); and
- Contributed services (e.g., in kind, royalty, gain share).

These revenue streams are more or less the same as in the current situation. The impact of MSaaS on the overall revenue and on the balance between the revenue streams is not yet clear. However, the expectation is that MSaaS will increase the overall M&S revenue due to improved availability and accessibility.

Current Customers of M&S products pay for the product (including tailoring, integration, interest charges, acquisition and contracting), lifecycle maintenance (licenses, technical support), hardware, facilities (including energy and cooling) and cost of operators (e.g., instructors, maintainers).

The following payment models are used:

- **Fixed pricing:** list price, product feature dependent, customer segment dependent, volume dependent.
- **Leasing:** fixed price or pay-per-use, product feature dependent, customer segment dependent, volume dependent.
- **Cost + incentive:** either including or excluding facility and operator costs.

Automated compensation for background Intellectual Property (IP) that is used in derived work is an emerging technology. This 'compensation in perpetuity' may allow fractional payment for use of IP thus permitting the tech stack and its components to move freely from one service to another.

Customers are willing to pay on competed price (value for money, best value for money), but the trend in civilian business and industry is towards more flexible payment models and dynamic pricing: subscription, pay-per-use, per-sale.

The MSaaS approach can include fixed pricing but is more amenable to leasing or pay-per-use models. The pay-per-use model has benefits for customers but may also offer opportunities for vendors to generate new revenue: customers that require specific (high-end) tools or services relatively rarely may now consider employing it and pay-per-use during a limited time instead of doing without or make-do with an improvised solution.

3.0 PROCUREMENT AND GOVERNANCE

3.1 Procurement Considerations

The MSaaS approach will need acceptance of a new way to meet user's M&S requirements. It moves away from traditional development cycles and contracting procedures but will still maintain the need for value for money. An M&S ecosystem driven by MSaaS, modelled around commercial app-based ecosystems, would provide greater choices of models and simulations, foster competition as well as collaboration amongst the ecosystem stakeholders, and tools to discover, compose, and execute efficiently and securely the required model, simulation, or synthetic environment.

3.2 Funding Models

The funding model for M&S as a Service will need to address different types of licensing and payment methods. Paying for M&S services within NATO MSaaS will be different than how it is presently done. Since we are moving away from actual purchases of hardware and software and instead are paying for a "Service", a service payment model will apply; such that payments for service will be paid out as part of the operating or in-service costs rather than the approach of capital purchase of bespoke hardware and software through the traditional acquisition phase. Additionally, this would include modern ecosystem mechanisms that provide on-line on-demand methods of delivery and payment such as:

- App store, including micro-payments: The As-you-go consumption based payments will make the funding of the NATO MSaaS somewhat different than the traditional government contract.

- Pay-per-use: the transfer of funds from the end consumers within the MSaaS community to the NATO managing body will need to be well-defined, since a micro-payment for "service" usage will be more appropriate to meet the demands of more frequent and flexible transactions take place between the provider, supplier, and consumer in relation to provisioning and accepting "services".
- Open source, possibly with contributions in kind (e.g., additional functionality added by users).
- Subscription: to meet the warfighters needs for services on demand, a phased approach is recommended to fund the establishment through a subscription model.
- On-line contracting.

To guarantee the uniformity of readiness, NATO MSaaS should establish a Steering Committee ("SC") to assist in the governance and voting on certain service fees above the usage fees during sustainment of the MSaaS Ecosystem. The SC will have a support team that provide support services to track and manage licensing as well as legal services to ensure compliance with operating in such a manner, e.g., Data Protection Laws. Many of these services are not new in the everyday commercial world.

Initially it will be a NATO subsidized effort, starting with a phased migration to adopt the new business model by establishing new default services to be readily available off the platform ecosystem, it will be augmented with the suppliers or providers to port legacy defence M&S capability into MSaaS if such models do not exist in the ecosystem.

The delivery options for the required M&S products and services will also need to accommodate local restrictions (e.g., security of physical asset), distributed (e.g., to address team, joint or coalition requirement) or a mix of the two (hybrid).

3.3 Typical Governance Approach

In order to ensure a successful cloud purchasing and usage across NATO nations, two practices must take place. First, a review and determination on contractual terms and conditions should be performed. Current NATO Acquisition Regulations state that contracts for procuring commercial items must include only those contract clauses required to implement provisions of law applicable to the acquisition of commercial items or determined to be consistent with customary commercial practice. Therefore, NATO and national contracting offices needs to ensure they have additions to customary commercial agreements that focus on the goal of avoiding inconsistencies between commercial regulation and NATO regulations. This must be accomplished without unduly burdening industry or creating actual risks from changes to commercial practices. Second, NATO nations will be accountable for managing the risk to their area of responsibility and that responsibility cannot be outsourced via Service Level Agreements. Many recommendations point to the potential benefits of clarifying roles and responsibilities, establishing clear performance metrics, and implementing remediation plans for non-compliance and security incidents. An important element of acquiring cloud services is clarity in what services a cloud provider performs and at what level. Such governance, architecture, and operational clarity would help NATO nations ensure services are performed effectively, efficiently, and securely.

In accordance with Customer Service Level Agreements (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 and services, 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 governance approach will need to include:

- Lifecycle management of products, services, and apps – addressing the roles and responsibilities for each stage of the MSaaS sourcing lifecycle;

- Configuration management;
- Change Management;
- Risk Management;
- Compliance and Accreditation;
- Data Management;
- Business Continuity Plan;
- Disaster Recovery Plan; and
- (Security) Incident Management.

3.4 Security

Access, commercial and defence security will be essential to the success of taking an MSaaS approach. This will include but is not limited to the following security measures:

- User Management;
- Authentication;
- Single Sign-On;
- Accreditation;
- Licensing and IP protection;
- Data (encryption at rest, encryption in transit), cross-domain-solution? data in use by services?
- Cyber security; and
- (Security) Incident Management.

There are many aspects of "security" that must be considered when implementing MSaaS covering the models, products, and systems to be implemented across the network and computing devices (local and remote/cloud). The use of enablers, such as cloud computing, smart communications (e.g., 5G), autonomy, etc., is not unique to MSaaS, as many other defence capabilities are looking to leverage these commercial-sector technologies, which provides opportunities for lessons identified in various aspects of security. This section serves as a summary of key considerations across various facets of security, but the topic will require more exhaustive guidance as the MSaaS Ecosystem evolves. Furthermore, while NATO will identify best practices and requirements for Cybersecurity and Information Assurance, individual nations will likely have their own (additional) requirements, which must be considered in an MSaaS implementation. Every MSaaS implementation will be unique, so there is no one size fits all and the set of security requirements needs to be reviewed/assessed periodically.

3.4.1 Cybersecurity Need

We need to identify related Cybersecurity frameworks and roadmaps that will affect the selection of key MSaaS technologies and facilitate network interoperability at future milestones as well as identify the importance and dependencies of obtaining security accreditation of key services and technologies. At the same time, we need to implement and enforce cybersecurity policies for M&S services. Overall, cybersecurity is about Securing and Protecting the "DATA" and functionality, through a secure Framework.

M&S products are highly valuable to NATO and military organizations, and it is essential that M&S products, data, and processes to be under cyber hygiene with an acceptable security posture and at the same time,

conveniently accessible to a large number of users whenever and wherever needed. 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.

Ensuring the proper cybersecurity is intrinsically related to the cloud computing service model (Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)) and to the deployment model (Public, Private, Hybrid, or Community) that best fits the Consumer's mission and cybersecurity requirements. The Consumer must evaluate the particular cybersecurity requirements in the specific architectural context and map them to proper security controls and practices in technical, operational, and management classes. While the Cloud Security Reference Architecture [9] possesses a rich body of knowledge of general network security and information security, both in theory and in practice, it also addresses the cloud-specific security requirements triggered by characteristics unique to the cloud, such as decreased visibility and control by consumers. Cloud security frameworks including information management within an infrastructure shall support the cloud implementers, providers, and consumers. However, MSG-164 recognizes that a more tailored approach may be needed to exploit MSaaS specific capabilities and proposes to develop additional guidelines as part of the work.

3.4.2 Cybersecurity Overview

The Committee on National Security Systems Instruction (CNSSI) Glossary (CNSSI-4009) defines cybersecurity as "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

The objective of cybersecurity is to make sure all products and access controls to the products and services are secured and protected. The MSaaS ecosystem should implement a secure information/data flow exchange, access controls, eliminate attack vectors, secure hygiene and balanced protection of the Confidentiality, Integrity, and Availability (CIA) of data in a cloud environment (Figure 3). At the same time, MSaaS needs to give flexibility and freedom of the development lifecycle.

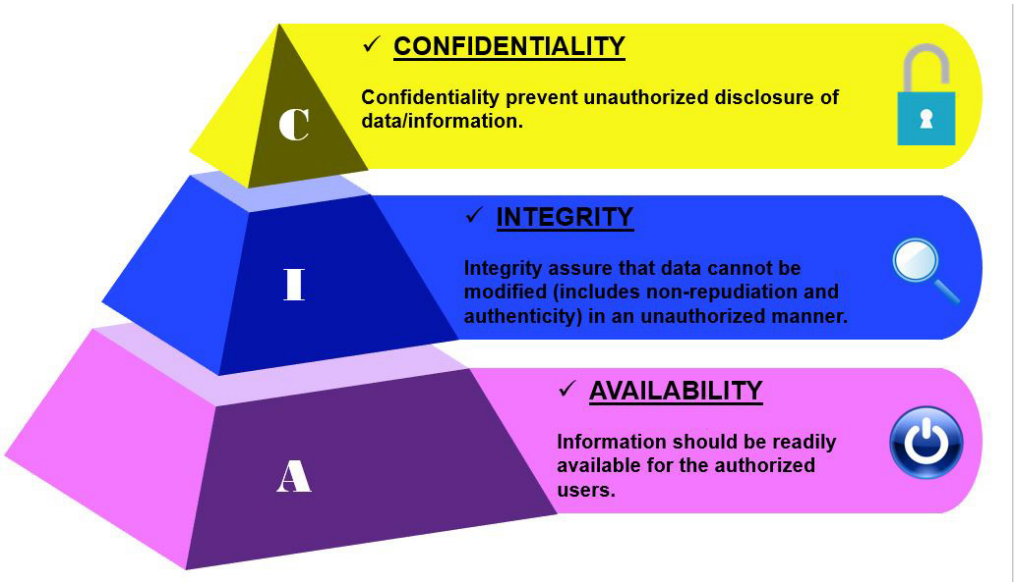

Figure 3: Confidentiality, Integrity, Availability.

The correct cybersecurity implementation will safeguard our stakeholders by employing a secure posture, for accessed services, data, account information, classification, classification upgraded by aggregation, and Personally Identifiable Information (PII).

The correct cybersecurity implementation will ensure Confidentiality, Integrity, and Availability (CIA) of simulation data while provisioning multiple synthetic sessions simultaneously to a widely distributed audience, while customizing the stream dynamically based on security access and need to know according to credentials.

There are multiple layers of cybersecurity (e.g., cryptography, firewalls, access control, etc.).

3.4.3 Cybersecurity Challenges

Cybersecurity challenges are different when we move the services and products to the cloud environment. Concerns include the complications of multiple organizations having access to our products and more importantly, our data. We cannot manage what we cannot control, and we cannot control what we do not manage. Questions include:

- Who will Monitor, Audit, Report and Risk Manage the data?
- How do we effectively protect/secure the data?
- Where does the protected data reside and where is it stored?

Cybersecurity Assessment is a process intended to ensure that software and/or data to be deployed in a cloud or other IT) environment has a specific level of cybersecurity. It is a process that reviews the software and/or data from different perspectives. The overall goal is to ensure a high level of CIA. At the end of the process, an assessment must be made as to whether the software (simulation service) and/or data is safe enough to be hosted in the cloud environment or not. While 100% security is highly unlikely, this process contributes to a consistent and reproducible security analysis that will increase IT security. The process is not a guide to the secure operation of a cloud infrastructure, but only to ensure that only security-tested software is imbedded into the cloud environment.

Guidelines need to be developed and implemented covering:

- Use of secure coding best practices and code analysis.
- Establish an acceptable common criteria threshold level for incoming services. These criteria will ensure the product is assessed for risk management in the concepts of CIA tenets.
- Metadata for security and classification tagging.
- Assurance that the data/information is trustworthy and accurate.
- Data confidentiality that limits access to information/data.

The Access Control Plan defines the policy and associated access security controls that allows the MSaaS IT to manage risks from information asset access. It gives users access to the networks and systems they need, while restricting access to those they do not need by creating a unique digital identity.

The organization considering MSaaS (or any other IT) implementation, needs to evaluate the acceptable level of risk. A balance has to be found between security and costs. In addition, a process should be in place to mitigate the remaining risk to the smallest possible level of impact.

3.4.10 Additional Considerations

While the aforementioned Cybersecurity and Information Assurance considerations are paramount, discussions on licensing and Intellectual Property will also be required as the MSaaS Ecosystem implements service discovery. Furthermore, the implementation of Cross Domain Security solutions will further drive security considerations for future MSaaS implementations. In execution, it is highly likely that not all MSaaS users will have access to the same services, data and applications and security will play a key role in how this is enabled.

Nations and Organizations have to assess risk and balance 'risk appetite' with business benefits. This a continuous process as recommended in Control Objectives for Information and Related Technologies version 2019 [11] and needs to follow national policies and regulations. Overall Risk management is broader than Cybersecurity and is addressed in more detail in guidance documents [12].

4.0 IMPLEMENTATION PLAN

Implementing the Allied Framework for M&S as a Service will result in various benefits and improvements for the different stakeholders. However, stakeholders that 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 Section 2.6 of MSG-131 [13]. The section concludes with a proposed way-ahead to implement the MSaaS ecosystem through a phased approach that builds on the results from MSG-136 and MSG-164 while addressing the identified challenges and risks.

4.1 Improvements and Benefits

Implementing the Allied Framework for M&S as a Service will (ultimately) result in various benefits and improvements for the different stakeholders. The MSaaS Business Model is designed to:

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 at remote locations.
- **Increased efficiency and productivity for defence applications:** Due to the increased access to a larger variety of M&S products and 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 defence use of M&S.
- **Improved quality:** The MSaaS Portal creates transparency about existing products and 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.

Increase efficiency in a stable and established situation:

- **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 implementation of HICON/LOCON products.

- **Reduced reliance on SMEs and available expertise:** In the MSaaS concept, much of the required knowledge and expertise needed to deploy simulations today will be provided as a service in the future. Therefore, reliance on (in-house) SMEs can be significantly reduced.
- **Increased re-use 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 re-use 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 the use of 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, accessibility, etc.

4.2 Implementation Risks

Stakeholders that implement the proposed concept into their organizations will also face risks and some major challenges. The following general (i.e., not defence-specific) risks associated with service-based M&S approaches have been identified as:

- 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. Applications relying on specific hardware (e.g., Mock-ups) may be hard to integrate and can't be scaled up as needed. Some M&S applications may also not have the appropriate User License Agreements in place for cloud deployment.
- 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.

MSaaS performance metrics will need special attention in the discussion on risk. Performance aspects will typically be included in the SLA. The MSaaS Concept of Deployment will have to provide guidelines for these metrics and some example metrics should be provided and included in the SLA Template. In general, MSaaS metrics for every MSaaS instantiation will be specific or tailored.

Existing methodology can serve as starting point for metrics selection. Performance metrics and how to implement them are found in COBIT 2019. COBIT 2019 is a general framework created by International Systems Audit and Control Association (ISACA) and defines a set of generic processes for IT management. Every organization can define metrics for its specific situation or type of implementation using this framework as a guideline.

Specific performance metrics can be captured through all major public MSaaS providers' logging tools as well as possible from deployable logging software for those NATO components that will be deployed on-premises. Relevant metrics for simulation services are:

- Latency: The simulations or other training tools should not be delayed as to cause issues with training individuals or groups. This latency is variable depending on the requirements of the individual tool.
- Scalability: The core components selected should be able to scale to meet the demands required and expected when MSaaS is adopted in a rapid and extensive manner to enable training or decision support applications.

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 Commercial-off-the-Shelf (COTS) products. Note that it may be possible for some legacy/COTS products to act as an MSaaS by encapsulating it in a wrapper. There can be additional or transition cost for legacy systems.
- 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 (IPR, security.).
- Unwillingness of companies to move to a pay-per-use or other required funding 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.

Appendix 1 provides several high-level examples of the value proposition and perceived risks for operational use cases in the identified application segments.

4.3 Interoperability of Allied and National MSaaS Implementations

The objective of the Allied Framework for MSaaS is to create interoperability between different MSaaS implementations and make sure they can interoperate with each other. Implementations may include the following:

- MSaaS implementation on NATO level.
- MSaaS implementations on national level.
- Mission-specific MSaaS implementations.
- MSaaS implementations on different security levels (e.g., NATO Unclassified, NATO Secret).

The market for a cloud ecosystem is large, with many providers offering a wide variety of cloud services. Understanding the interoperability and portability "of what" is the necessary first step of planning and designing for the use of any cloud service. Clarifying the specific interoperability and portability concerns accelerates identification of the "best fit" options and potential development of solutions. Interoperability can be defined as a measure of the degree to which diverse systems or components can work together successfully. More formally, IEEE and ISO define interoperability as the ability for two or more systems or applications to exchange information and mutually use the information that has been exchanged. In the context of cloud computing, interoperability should be viewed as the capability of public cloud services, private cloud services, and other diverse systems within the enterprise to understand each other's application and service interfaces, configuration, forms of authentication and authorization, data formats, etc. in order to work with each other. In cloud computing, the most significant interacting components are those which belong to the cloud service customer which interact with components of the cloud service provider. The nature of the interaction is a network connection using a prescribed interface or API as defined by the Reference Architecture [4]. There are typically multiple separate interfaces, each dealing with a different aspect of the cloud service. For example, there are the functional interfaces of the cloud service itself, authentication and authorization interfaces, interfaces for administration of the cloud services, and business interfaces for billing and invoicing. The ideal of interoperability is that the interfaces are standardized in some way – i.e., they are interoperable – so that the customer can switch to another cloud service provider with minimal impact on the customer's components and services.

In order to enhance interoperability of systems and maintain a baseline of business operations, Service Level Agreements are required. A Service Level Agreement defines the level of performance expected from a service provider, how that performance will be measured, and what enforcement mechanisms will be used to ensure the specified levels are achieved. In the NATO acquisition context, the need for these agreements will be incorporated via contract clauses and quality assurance provisions. In the early stages of procuring services for MSaaS, these agreements will be critical elements of negotiation with suppliers. Where a cloud solution is deployed by a vendor, a Service Level Agreement (SLA) will be in place that provides the agency with continuous awareness of the confidentiality, security, and availability of its data.

4.4 MSaaS Roadmap

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 implementations. It is thought that scaling across particular

M&S communities (i.e., Training, Test and Evaluation, Concept Development and 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 national ecosystem. While these aren't specifically related to the MSaaS reference architecture or business model, 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.

The diagram in Figure 4 depicts the proposed way-ahead to implement the federated MSaaS ecosystem through a phased approach that builds on the results from MSG-136 and MSG-164 while addressing the challenges discussed above.

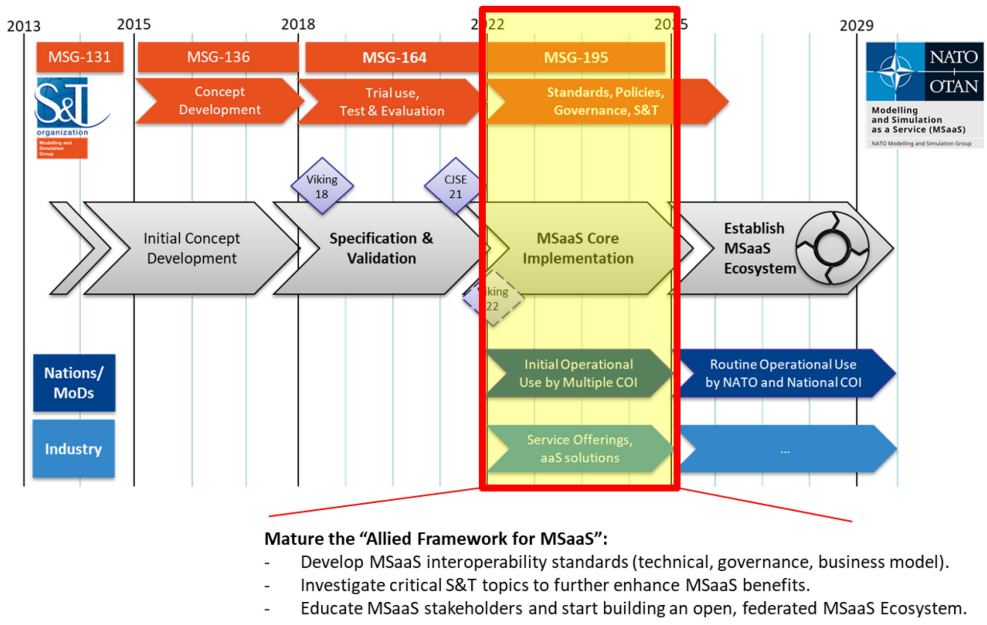

Figure 4: MSaaS Implementation Plan.

The next two phases (3 and 4) that are foreseen in NATO MSaaS Capability roadmap, following completion of the initial concept development (phase 1) and the specification and validation (phase 2) of the concept, will need different funding methodologies:

- **MSaaS Core Implementation phase –** This represents the initial establishment phase of the NATO MSaaS Capability. MSaaS will be populated with new and/or existing applications and evaluated by the users in order to determine most low-hanging issues that can be resolved in order to expand both the number of applications, datasets, protocols available on the MSaaS. The capability will be used in different Communities Of Interest (COIs) thus allowing all stakeholders to gain experience and improve MSaaS through lessons learned. Specific remaining technical or organizational gaps will be addressed by NMSG task groups. Additionally, during this phase, a concurrent effort will continue to evolve MSaaS by researching emerging technologies, including AI, ML, various sophisticated encryption technologies, quantum computing, data-driven capabilities (authoritative data sources, federated datasets) and data-centric capabilities.
- **MSaaS Ecosystem growth phase –** This phase represents the longer term steady state of the MSaaS Capability where most existing applications, reference datasets, protocols and analysis tools have been moved or migrated to MSaaS and where newly developed applications will typically always be offered as a service rather than in the traditional business model format. To guarantee the uniformity of readiness, NATO MSaaS needs establishment of the initial starting conditions for these next phases (e.g., stabile set of technical standards and procedures) and guidelines to assist in the maintenance and governance (custodianship) of the ecosystem. The governance body and broader NATO Community will have to recommend a "best of breed" of current tools and provide those organizations or companies with "start-up" funds to move the tools to MSaaS and maintain and upgrade them for a set period of time.

In some cases, NATO Common Funded Projects may be suitable to fund the transition to MSaaS e.g., CAX systems to be used by NATO and many nations. In other cases, nationally or industry funded projects may be more relevant e.g., specific training systems for vehicles or weapons. These national/industry transition projects will follow NATO guidelines on MSaaS and work closely with the NATO MSaaS community. The NATO managing body will need to be in a well-defined framework different from the traditional government contract for sustainment of the Ecosystem.

5.0 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

The NATO MSaaS presents a fundamentally different way of procuring and paying for M&S products and services within the MoD/NATO. Traditional contracts with set upgrade and service contracts may no longer be a part for most of the components deployed. Outside of edge on-premises use cases, the payments for the business may be funded differently from today e.g., funded as part of the in-service or operational costs. This will be nation dependent. The As-you-go consumption based payments will make the funding of the NATO MSaaS somewhat consumer based within the MSaaS community. The NATO managing body will need to be well-defined, since a micro-payment for "service" usage will be more appropriate to meet the demands of more frequent and flexible transactions between the provider, supplier, and consumer in relation to provisioning and accepting "services".

As a means to facilitate migration towards the MSaaS business model that adopts micro-payments from potentially many different accounts to meet the war fighters needs for services on demand, a phased approach is recommended to fund the establishment of a platform ecosystem, through e.g., a NATO Common Funded Project which will eventually result in an ecosystem that will be self-sustained through usage fees to provision services.

The MSaaS development has followed a phased procedure:

- Initial concept development (phase 1).
- Specification and validation of the concept (phase 2).

The next following phases are expected to be:

- MSaaS Core Implementation (phase 3).
- MSaaS Ecosystem growth (phase 4).

5.2 Recommendations

Nations are recommended to:

- Issue guidelines on how to implement the MSaaS ecosystem and the proposed funding mechanism, including how to use the BM and the Canvas to gain understanding and determine at the National level the customer and supplier contributions.
- Initiate MSaaS Core Implementation phase plan in preparation for the MSaaS ecosystem growth phase (Steady state).

NATO is recommended to:

- Establish a NATO MSaaS Steering Committee to assist in the governance and maintenance of the (federated) MSaaS Ecosystem.
- Co-ordinate MSaaS with other on-going NATO and National M&S projects and initiatives (e.g., NexGen M&S, Federated Mission Network (FMN)).

6.0 REFERENCES

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

[2] NATO Strategic Foresight Analysis 2017. https://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf

[3] NATO STO, "Operational Concept Description (OCD) for the Allied Framework for M&S as a Service," STO-TR-MSG-136-Part-III, NATO Science & Technology Organization, Neuilly-sur-Seine, France, 2019.

[4] NATO STO: "Modelling and Simulation as a Service (MSaaS) – Technical Reference Architecture," STO-TR-MSG-164-II, NATO Science & Technology Organization, Neuilly-sur-Seine, France, 2024.

[5] NATO: AMSP-02 "Allied Framework for Modelling & Simulation (MSaaS) – Concept of Employment". Edition (A), Version 1. To be published.

[6] Osterwalder, A. and Pigneur, Y., Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers, 2010.

[7] NATO STO: "MSG-080 Security in Collective Mission Simulation (CMS)," STO-TR-MSG-080, NATO Science & Technology Organization, Neuilly-sur-Seine, France, 2014.

[8] NATO STO: "MSG-165 Reference Architecture for Mission Training through Distributed Simulation (MTDS)," STO-TR-MSG-165, NATO Science & Technology Organization, Neuilly-sur-Seine, France, 2021.

[9] NATO: AMSP-01 NATO Modelling and Simulation Standards Profile. Edition (D), Version 1. NSO, 2018.

[10] National Institute of Standards and Technology: Cloud Security Reference Architecture, https://bigdatawg.nist.gov/_uploadfiles/M0007_v1_3376532289.pdf

[11] International Systems Audit and Control Association (ISACA)'Control Objectives for Information and Related Technologies version 2019; https://www.isaca.org/cobit

[12] ISO31000 Risk Management. https://www.iso.org/iso-31000-risk-management.html

[13] NATO STO: "Modelling and Simulation as a Service: New Concepts and Service Oriented Architectures, " STO Technical Report TR-MSG-131, NATO Science & Technology Organization, Neuilly-sur-Seine, France, 2015.

[14] MC-0583 (Final), MC Policy for NATO Concept Development and Experimentation, 04 October 2010. http://www.act.nato.int/images/stories/events/2011/cde/rr_mc0583.pdf

Appendix 1: EXAMPLES OF OPERATIONAL USE CASES

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

1A.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.

Collective Training: Collection of INTEL Information	Customer	Users	Provider	Supplier	Required MSaaS Services
Example	NCIA	JWC, JFTC	NCIA ("NATO Cloud")	Industry, etc.	Joint Simulation, INTEL Report Service, UAV Full Motion Video STANAG compliant, etc.
MSaaS Advantages	• Access to shared information: the training audience could access to INTEL information through a unique service. Input data are collected by multiple and independent services. The INTEL information could be provided on multiple supports (video, military formatted message, raster, etc.) and filtered as needed. • On-demand access: the access of INTEL service is available freely for many requesters.				
MSaaS Challenges	• The service of shared INTEL information should integrate a security aspect to be compliant with the level(s) of data classification. A mechanism of authentication should be provided too in aim to filter the access of data according to the profile of the requester ("need to know"). • The merge of INTEL information needs automatic tools and process to be integrated as a lone service in a MSaaS capability (e.g., artificial intelligence).				

1A.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.

Training on Team Level: FAC	Customer	Users	Provider	Supplier	Required Capabilities
Example	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.
MSaaS Advantages	• Distributed access: the training audience of FAC is sometimes not located in the same site (pilots in airbase, FAC in special force center, etc.). MSaaS capability could offer a set of centralized services to access to the common synthetic environment (terrain, support of communication, etc.).				
MSaaS Challenges	• Provide realistic CGF service if one partner (pilot or FAC) is not available during a distributed exercise (automatic behaviors, artificial intelligence, etc.)				

1A.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.

Training on Individual Level: Cultural Awareness	**Customer**	**Users**	**Provider**	**Supplier**	**Required Capabilities**
Example	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
MSaaS Advantages	• On-demand access: The training audience could access to the Cultural Awareness where they want (an access to network is mandatory), when they want (24/7 access) and to what they want (selection of a specific training activity).				
MSaaS Challenges	• Provide a realistic service of Cultural Awareness to avoid repetitive lessons boring the training audience and the feeling to talk to a computer and not a human.				

1A.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 [1].

Support to Operations Planning	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
MSaaS Advantages	• Reducing disturbance inside the legacy system: Access to multiple support services without installing and setting components in the local C2 system.				
MSaaS Challenges	• To provide a remote access to the MSaaS capability (rear operating base or home base) • To deploy a specific MSaaS capability in the theater of operations.				

1A.5 CONCEPT DEVELOPMENT AND EXPERIMENTATION

CD&E is one of the tools that drive NATO's transformation by enabling the structured development of creative and innovative ideas into viable solutions for capability development [14].

This use case addresses an MSaaS environment for future military capabilities development in order to provide flexible services to develop new concepts and to experiment it.

CD&E	Customer	Users	Provider	Supplier	Required Capabilities
Examples	Dutch MoD	Capability Developers, Training audience and organizations	KIXS MSaaS Cloud (Simulation Battle Lab)	Defence KIXS/SIM Organization and TNO and Industry	Scenario Development Services, CGF service, Analysis services and AIS Service, Terrain Service.
MSaaS Advantages	• On-demand access: The analysis team could discover and access different solutions for composition and assessment. • Composition of services.				
MSaaS Challenges	• Prevent information leakage between different (competing) providers. • Consistency between models/simulations when scaling up from constructive to virtual. Note that this issue is potentially more problematic in MSaaS context where more suppliers/providers may be involved. • Secure Access (IdAM). • Bandwidth availability during execution.				

1A.6 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 fulfil its missions [1].

Procurement/ Acquisition	Customer	User	Provider	Supplier	Required Capabilities
Example	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
MSaaS Advantages	• Calculation support: A service of massive calculation (data farming) could be shared and automatically adjusted according to the peak of analysis activity. • On-demand access: The analysis team could access different vendor's solutions for composition and assessment.				
MSaaS Challenges	• The services of preparation, calculation and analysis should integrate a security aspect to be compliant with the level(s) of data classification. • Prevent information leakage between different (competing) providers.				

Appendix 2: STAKEHOLDER ROLES AND EXAMPLES

2A.1 EXAMPLE STAKEHOLDER ROLES AND INTERACTIONS

The Customer (ACO) has requested a NATO NRF Exercise (Steadfast Joiner) from Provider (ACT). Provider (ACT) submits requirement to User (JWC) to execute the exercise. User (JWC) uses simulation services from Suppliers (Roland) provisioned by the Provider (ACT) to enable the exercise.

Customer: NATO ACO

Provider: NATO ACT

User: JWC

Supplier: Roland (JTLS Simulation)

The interactions between the various stakeholders are illustrated in the following example (Figure 2A-1):

- Customer and User collect/define operational needs and gathers requirements together with User.
- User states Capability Needs to Customer (e.g., requirements for simulation support for training and/or exercises).
- Customer makes contract/license agreement about capabilities with Supplier and/or Provider.
- MSaaS Supplier deals with Provider to service Customer in accordance with the contract/license agreement and Provider makes a contract with Supplier.
- Provider deals with Suppliers License agreement.
- MSaaS Provider opens / sets up Environment for User.
- User does training / exercise in Simulation.
- User provides feedback to Customer and MSaaS Provider.
- MSaaS Provider provides feedback to Supplier.

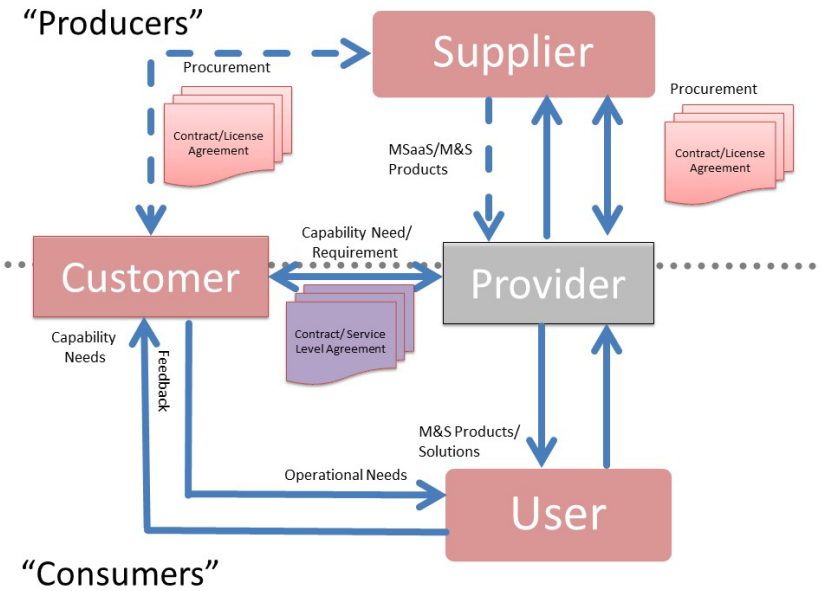

Figure 2A-1: Stakeholders and Interactions.

2A.2 CUSTOMERS

The Customer is the acquirer of M&S services, for example a defence organization with an operational need (e.g., training, mission planning, acquisition), and are the budget holder.

The Customer will assist the User by capturing the capability needs based on the operational needs and breaking these down in technical requirements. In some cases, the Customer will perform a Trainings Needs Analysis (TNA) before sharing the requirements with the Service Provider.

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.

According to the definitions where Customers are Defence organizations with an operational need (e.g., training, mission planning, acquisition), and is the budget holder. Possible Customers in the NATO MSaaS BM are identified with the following organizations:

- NATO HQ SACT, Allied Command for Transformation (ACT), Joint Warfare Centre (JWC), Joint Force Training Centre (JFTC);
- ACO (Mons), SHAPE HQ, SACEUR, Joint Force Command (JFC), Land, Air and Maritime Components;
- NATO Support Procurement Agency (NSPA);
- NATO Communication and Information Agency (NCIA);
- NATO HQ Infrastructure Committee (NOR);
- Centres of Excellence (e.g., M&S, Cooperative Cyber Defence);
- Nations (NATO, Partners MODs): Simulation Centres, Armed Forces, Other Organizations;
- Science & Technology Organization (STO);
- NATO Force Structure.

2A.3 PROVIDERS

The Provider makes M&S products and services (including integrated or composed services such as executable simulations) available to Users of the Allied Framework for MSaaS in accordance with Customer SLAs. The Provider has the responsibility for the composition and integration of M&S services in accordance with Customer requirements.

Service Providers will engage with Suppliers to acquire and integrate M&S products and services 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.

Possible Providers in the NATO MSaaS BM are identified with the following organizations:

- NCIA;
- JWC /JFTC;
- STO (e.g., Provider for MSaaS experimentation services);
- National Defence IT HQ'S (e.g., ITA MOD C4 HQ), Simulation Centres (e.g., Italian Army Simulation Centre), Other Organizations (e.g., Dstl UK);
- INDUSTRY (e.g., Amazon, Google, Defence Enterprise, IT Services Provider); and
- M&S COE (e.g., Provider for MSaaS experimentation services).

2A.4 USERS

The User is the consumer of M&S services. 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.

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 two User sub-categories Simulation Users and Operational users. Possible Users in the NATO MSaaS BM are identified with the following organizations:

- NATO Training Centres (JWC, JFTC);
- JALLC;
- National Centres (Simulation, Wargaming, Analysis, Scientific);
- NATO COE'S (M&S COE, etc.);
- NATO COMMAND HQ'S/NATO Force Structure;
- NDC;
- NCIA;
- STO (CMRE);
- NATO Schools (e.g., NATO School Oberammergau);
- National Defence and Armed Forces HQs; and
- Industry.

2A.5 SUPPLIERS

The Supplier supplies M&S services to the Provider as part of the Allied Framework for MSaaS, for example via a procurement or a license agreement.

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.

Possible Suppliers in the NATO MSaaS BM are:

- Industry (Hardware and Software manufacturer and producers) Small, Medium Companies and Large Enterprises;
- Academia;
- Government National Organizations (Defence/Research Labs);
- NCIA; and
- STO (e.g., RTG activities).

2A.6 STAKEHOLDER SEGMENTS

The Stakeholders Segment Operational needs are related to the NATO Masterplan Application Areas:

- Operations (Operational Planning, Analysis, Decision Making);
- Capability Development (Defence Planning, Concept Development and Experimentation);
- Mission Rehearsal;
- Training And Education (Exercise); and
- Procurement.

2A.7 SUMMARY OF STAKEHOLDERS AND ROLES

Typical Stakeholders in NATO and their main roles are illustrated in Table 2A-1.

Table 2A-1: Typical Stakeholder Roles Within NATO.

Stakeholder	General Description	Stakeholder Role			
		Customer	Provider	User	Supplier
Academia	Conducts M&S-related research and development.				x
ACO (JFC's, CC's, NRF, Operations)	Provides operational requirements for M&S planning tools, decision-making tools, operational support tools and training tools.	x			
ACT (incl. JWC, JFTC, JALLC)	Facilitates and leads development of capabilities and interoperability for medium and long-term solutions.		x		
	Provides Bi-Strategic-Commands military requirements to NMSG.	x			

Stakeholder	General Description	Stakeholder Role			
		Customer	Provider	User	Supplier
ACT (incl. JWC, JFTC, JALLC) (cont'd)	Responsible for Defence Planning, CD&E, training and exercise, and analysis using M&S solutions.			x	
ACT/NTG	Provides training standards.	x			
Industry (e.g., Amazon, Google, IT Services Provider)	Develops M&S solutions.				x
	Using M&S to reduce risk to equipment design and lifecycle.	x		x	
M&S COE	Provide resources and requirements for M&S capabilities. Use resources as Customer or User.		x	x	
NATIONS (Including NATO and Partner Nations)	Provide resources for the capabilities.		x		x
	Provide requirements for the capabilities.	x			
	Final users of most of the capabilities provided by implementation of MSaaS.			x	
	Provide most of the assets/ capabilities needed to implement this MSaaS.		x		x
NATO HQ (i.e., NOR)	Provides requirements and guidelines.	x			
NATO main armament groups	Provides requirements and studies.	x		x	
NATO schools	Provides requirements for M&S tools for education.	x		x	
NCIA	Provides M&S solutions.		x		x
	Provides communications and IT support.		x		
	Provide studies and exercise support.			x	
NIAG	Provides studies and solutions.			x	

Stakeholder	General Description	Stakeholder Role			
		Customer	Provider	User	Supplier
NMSG	Military operation requirements subgroup.	x			
	Creates and oversees working groups in support of the creation of Long / Medium / Short Term M&S Solutions and Standards.				x
	MSCO maintains the NATO simulation resource library.		x		
NSPA	NATO Support and Procurement Agency. Support to Operations and Exercises, Systems Procurement and Life Cycle Management.	x			
Other COEs (e.g., Cooperative Cyber Defence)	Provides requirements and studies.	x		x	
Standards Development Organizations	Develop international standards.				x
STO Panels	Creates and oversees working groups in support of the creation of Long / Medium / Short Term M&S Solutions on specific areas.			x	
STO-CMRE	Develops Maritime Research and Models (NURC).				x
	Studies on future solutions.			x	
NDC	NATO Defence College.			x	

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-MSG-164-Vol-III AC/323(MSG-164)TP/1185	ISBN 978-92-837-2497-1	PUBLIC RELEASE

5. Originator

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

6. Title

Business Model for the Allied Framework for M&S as a Service

7. Presented at/Sponsored by

Developed by NATO MSG-164.

8. Author(s)/Editor(s)	9. Date
Multiple	April 2024
10. Author's/Editor's Address	**11. Pages**
Multiple	54

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

MSaaS; M&S as a Service; Simulation; Training

14. Abstract

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-164 developed the technical and organizational foundations to establish the Allied Framework for M&S as a Service within NATO and partner nations.

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

DANEMARK
Danish Acquisition and Logistics Organization
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

FINLAND
Ministry for Foreign Affairs
Telecommunications Centre (24/7)
P.O Box 176, FI-00023 Government

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

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"

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

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 01 Liptovský Mikuláš 1

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

SUEDE
Regeringskansliet,
Attn: Adam Hidestå
RK IF AR 5
S-103 33 Stockholm

TCHEQUIE
Vojenský technický ústav s.p.
CZ Distribution Information
Mladoboleslavská 944
PO Box 18, 197 06 Praha 9

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

CZECHIA
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

FINLAND
Ministry for Foreign Affairs
Telecommunications Centre (24/7)
P.O Box 176, FI-00023 Government

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 01 Liptovský Mikuláš 1

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

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

SWEDEN
Regeringskansliet, Attn: Adam Hidestål
RK IF AR 5
S-103 33 Stockholm

TÜRKIYE
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 978-92-837-2497-1