MSG-168 Lecture Series on Modelling and Simulation as a Service (MSaaS)

1. Need and Motivation for MSaaS

5. MSaaS Benefits and Achievability

7. MSaaS Business Model Development

Bharat Patel
DSTL, UK MoD

bmpatel@dstl.gov.uk

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.

In an increasingly complex, competitive and connected world, the challenge is not responding to what we know today, but rather preparing for what tomorrow might bring. The future defence and security users will need a more rapid approach with greater scope to model and simulate the future operating environments. The Modelling and Simulation as a Service (MSaaS) Concept was developed to enable an Ecosystem and meet this need.

In this paper, I will be presenting the following topics:

- *Need and Motivation for MSaaS*
- *MSaaS Benefits and Achievability*
- *MSaaS Business Model Development.*

1.0 NEED AND MOTIVATION FOR MSAAS

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 have to be integrated seamlessly in future computer information systems capabilities to ensure increased responsiveness, efficiency, affordability, interoperability and reusability.

The need to be more responsive is driven by the future trends in an increasingly complex, competitive and connected world that will define the future threats and hybrid environments NATO defence forces will operate. The challenge for these forces is not in responding to what we know today, but rather preparing for what tomorrow might bring.

The future trends are defined by the NATO Strategic Foresight Analysis (SFA) 2017 (currently being updated), which provides a wide-ranging shared understanding of the future security environment. It describes the future NATO expects to 2035 and beyond. The SFA depicts the future as political, human, technological, economic, and environmental trends. Where trends may move in diverging directions, SFA provides an alternative view to maintain objectivity.

So the M&S needs will be much broader, characterised by not only traditional warfare but including other elements that may impact the security of NATO and Nations. The M&S 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 our M&S are too focused on traditional warfare and developed through traditional procurement cycle that is unlike to meet the future needs of M&S users.

Such an increase in M&S requirement brings into the question of affordability as defence budgets are unlikely to increase or even prioritised for M&S capability. Increasing the efficiency and reusability across NATO and its nations will make M&S more affordable. To achieve this there will be the need for greater sharing of models and simulations to leverage investments, greater interoperability to compose the right simulation or synthetic environment quickly.

The motivation behind MSaaS originated from the science and technical (S&T) developments in the area of Service Oriented Architectures (SOA) – mainly in the commercial software development sector. It was considered to offer opportunities for providing M&S solutions that address the above shortfalls. The application of a “services” model to Modelling and Simulation, became known as “Modelling and Simulation as a Service” (MSaaS), and had 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.

More recently the motivation for MSaaS had been aligned to modernising defence through practices to match commercial practices (e.g. ecosystem, on-line on-demand at point of need) and exploiting commercial technologies (e.g. cloud computing, virtual reality, smart phones).

1.1 Characterising the Future

The political trends are characterised 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
- Greater public discontent and increasing challenges to governance.

The Human trends are defined by:

- Asymmetric demographic change, with ageing population priority over defence budgets, and developing nations’ youth unemployment and unrest
- Rapid urbanization, giving rise to resource scarcity and challenge to distribution of available resources
- Increasingly fractured and polarized societies
- Interconnected human networks, which brings both opportunities and challenges.

The Economic/Resources trends are characterised by:

- Globalization has opened markets and intensified economic integration, resulting in increasing influence of developing countries and straining natural resources

- Emerging markets shifting jobs to countries and regions with cheap labour, giving rise to eroding the economic base for the working middle class in Western countries, fuelling 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.

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

- Shape the social, cultural, and economic fabrics of our societies at all levels
- Offer enormous opportunities (not just to us but our adversaries), particularly offensive cyber, artificial intelligence (AI), autonomous systems, synthetic biology and human enhancement
- Bring new vulnerabilities and challenges as the world digitises
- Give rise to fake news
- 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 and addressing risk that these trends bring.

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.

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. The objective is to create interoperability between different MSaaS implementations and make sure they can interoperate with each other.

2.0 BENEFITS AND ACHIEABILITY

The implementation of MSaaS and the resulting ecosystem has the potential to accrue significant benefits provided the challenges of achieving MSaaS can be met.

The benefits would be:

- Greater Agility to meet the demands of fast-changing and complex defence and security environment, in particularly rapidly representing the future operational environments, representing full-spectrum of effects, and integrating real world data feeds

- Greater Effectiveness through using MSaaS to prepare agile force elements at high level of readiness, to carry out more comprehensive and immersive mission rehearsal, and to support operational decision when planning as well as during prosecuting missions or campaigns. In addition, MSaaS can better inform balance of investments amongst air, land, maritime, cyber, space, autonomous and information operations by supporting operational research or analysis, capability experimentation

- Greater Efficiency through MSaaS taking advantage of commercial practices such as on-line on-demand service based ecosystem, leveraging and adapting commercial technology much quicker, and de-risking capability development, test and evaluation and delivery.

MSaaS has the potential to not only provide significant enhancement to defence capability but also provides a faster, better and cheaper approach to the need of M&S for defence and security.

2.1 Efficiency Benefits

In summary, the MSaaS will provide time and efficiency savings through establishing and sustaining an on-line on-demand Modelling and Simulation as a Service (MSaaS) ecosystem of models, simulations, scenarios, data, tools and application services that will:

- Discover what we have/will have and what others have/will have that we can access and re-use, increasing the ability to take a “buy once use many times approach”.

- Compose rapidly, with reduced manpower and greater autonomy, the right synthetic environment or application for a required defence purpose such as training, exercises, mission rehearsal, or operational decision support.

- Execute the synthetic environment or application in a cloud-based environment to provide cost-savings against sustaining traditional computer-based infrastructure and communication systems.

More specifically efficient cost saving would be realised through:

M&S Software Cost Savings: The discovery service will provide an on-line searchable registry that will enable access to national investments and leverage international investments by our coalition partners. It will provide understanding of where models, simulations and data can be accessed from across defence and reused, as well as their fitness for the user’s intended purpose. It will also help to minimise duplication across defence simulation use. Ability to access a broad range of supplier capabilities through an “online simulation marketplace” will provide a rapid comparison of cost of competing products (licenses etc). The potential of “Pay per Use” business model could offer further efficiency savings as simulations are only paid for while they are in use. This business model would also allow MOD to recover M&S investments by offering them to other users through the marketplace.

Application Manpower Cost Savings: The move towards semi-automated/automated composition enables a novice user to rapidly assemble a simulation system capable of meeting their requirements. Automation and standards provide seamless integration of simulation services to meet that need. The ability to scale simulations to meet more complex scenario needs as well as direct connectivity to operational systems reduces the need to use role players to represent or interpret simulation responses. For example, it could substantially reduce exercise control manpower for a joint or combined HQ exercise by shortening the exercise planning cycle (potentially from months to weeks) and reducing the requirement for manned LOCONs and OPFOR control roles (potentially from 100s to 10s).

IT Infrastructure Cost Savings: The ability to deploy and execute a simulation on demand on secure cloud based hardware infrastructure, and then access it through web services, provides 24/7 access to simulation whenever/wherever. This reduces the need to procure specific hardware and comms solutions for defence simulation needs (though it is recognised that some niche hardware may still be required). This drives down the cost of deploying simulation infrastructure and personnel to defence events, such as in exercises, as the application can be accessed and executed remotely. The need to acquire or sustain large estate would be reduced too. Cloud based infrastructure and simulation architecture also provides greater resilience with better fault tolerance if simulation services fail, i.e. meaning less time spent on resolving simulation system issues.

2.2 Implementation Challenges

Implementing MSaaS and creating a sustainable defence M&S ecosystem will have technical challenges, which is the main focus for this lecture series. In addition to these technical challenges there are cultural, investment and reliance on commercial sector challenges:

- The culture change required will rely on innovative and creative thinking, novel approach to procuring capability.

- Defence budgets have not really recovered since "the peace dividend" divestments, and investment in M&S has to compete with other priorities, so the aim for MSaaS is to do even more with less money and people.

- Defence cannot compete for required technical skills with richer non-defence sectors, so defence M&S is dependent on leveraging technology developed by the commercial sector. Some of these technologies have short life span or morph into new technologies at rapid pace that cannot be matched by traditional defence decision, development and procurement cycles. So building resilience in adapting non-defence technology and preparing against adversaries with equal access to non-defence technology are both essential.

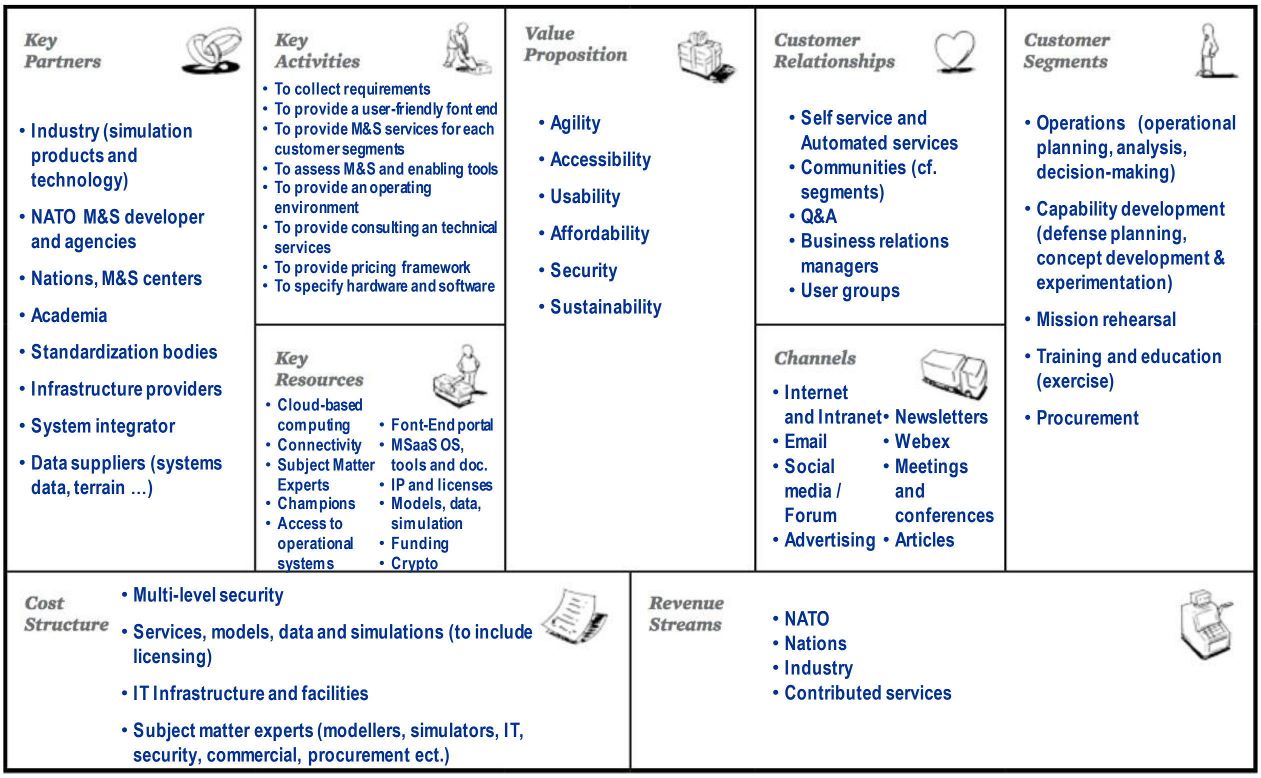
- Security challenges, both defence and commercial, are in line with those that defence needs to address more widely as it increasingly uses cloud-based or ecosystem approaches for defence business and operations.

3.0 MSAAS BUSINESS MODEL

The MSaaS Business Model is an integral part of the MSaaS Concept of Operations and is essential to sustain an M&S ecosystem. The Business Model 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 user's perspective. The development of the Business Model was initiated in the current phase of MSaaS capability development under the MSG-164 Task Group, so it is still work-in-progress.

3.1 Business Model Canvas

The purpose of the Business Model (BM) for the Allied Framework for M&S as a Service (MSaaS), developed based on the Osterwalder and Pigneur's (2010) third party funded Business Model Canvas, is to inform relevant stakeholders how the MSaaS will operate in the multi-government business space for the sharing of M&S technologies. The Business Model Canvas is a strategic management template for developing new or documenting existing business model. It is a visual chart with elements that describe the organizations value proposition, infrastructure, customers and finances. It assists organizations in aligning their activities by illustrating potential trade-offs. This document provides the elaboration of the MSaaS Business Model, Fig. below shows the visual chart. It shows typical defence and security perspectives that are being currently considered for the MSaaS BM.



Key Partners

- Industry (simulation products and technology)
- NATO M&S developer and agencies
- Nations, M&S centers
- Academia
- Standardization bodies
- Infrastructure providers
- System integrator
- Data suppliers (systems data, terrain …)

Key Activities

- To collect requirements
- To provide a user-friendly font end
- To provide M&S services for each customer segments
- To assess M&S and enabling tools
- To provide an operating environment
- To provide consulting an technical services
- To provide pricing framework
- To specify hardware and software

Key Resources

- Cloud-based computing
- Connectivity
- Subject Matter Experts
- Champions
- Access to operational systems
- Font-End portal
- MSaaS OS, tools and doc.
- IP and licenses
- Models, data, simulation
- Funding
- Crypto

Value Proposition

- Agility
- Accessibility
- Usability
- Affordability
- Security
- Sustainability

Customer Relationships

- Self service and Automated services
- Communities (cf. segments)
- Q&A
- Business relations managers
- User groups

Channels

- Internet and Intranet
- Email
- Social media / Forum
- Advertising
- Newsletters
- Webex
- Meetings and conferences
- Articles

Customer Segments

- Operations (operational planning, analysis, decision-making)
- Capability development (defense planning, concept development & experimentation)
- Mission rehearsal
- Training and education (exercise)
- Procurement

Cost Structure

- Multi-level security
- Services, models, data and simulations (to include licensing)
- IT Infrastructure and facilities
- Subject matter experts (modellers, simulators, IT, security, commercial, procurement ect.)

Revenue Streams

- NATO
- Nations
- Industry
- Contributed services

3.2 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 (Defense, and dual «civilian-military») marketplace.

3.3 Business Model Stakeholder Relationships

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

Customers

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

The Customer needs to consider the use of MSaaS capabilities available from the Allied Framework for MSaaS, typically via a Service Level agreement (SLA). Alternatively the Customer may procure M&S products and solutions from Suppliers via a contract or license agreement, to be subsequently made available to Users as part of the Allied Framework for MSaaS.

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

Providers

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

Users

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

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.

3.4 Procurement Considerations

The MSaaS approach will need acceptance of a new way for defence to meet users 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.

3.5 Supplier Business Model

The Supplier Business Model for M&S as a Service will need to address different types of licensing and payment methods. This would include modern ecosystem mechanisms that provide on-line on-demand methods of delivery and payment such as:

a. 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.

b. 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”.

c. Open source, possibly with contributions in kind (e.g. additional functionality added by users).

d. Subscription: to meet the warfighters needs for services on demand, a phased approach is recommended to fund the establishment through a subscription model.

e. On-line contracting

There will need to be support services that 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, suppliers or providers may need 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 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).

3.6 Typical Governance Approach

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, either already owned by defense 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:

1. Lifecycle management of services and apps – addressing the roles and responsibilities for each stage of the MSaaS sourcing lifecycle
2. Configuration management
3. Change Management
4. Risk Management
5. Compliance and Governance
6. Data Management
7. Business Continuity Plan

8. Disaster Recovery Plan
9. Incident Management.

3.7 Security

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

1. User Management.
2. Authentication
3. Single Sign On
4. Accreditation
5. Licensing and IP protection
6. Data (encryption at rest, encryption in transit), cross-domain-solution?, data in use by services?
7. Cyber security.
8. (Security) Incident Management.

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.

3.8 Improvements and Benefits

Implementing the Allied Framework for M&S as a Service will 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 on remote locations.

- **Increased efficiency and productivity for defence applications:** Due to the increased access to a larger variety of M&S services, it will be possible to create and use more complex and complete simulation services. This will contribute to an increase in the efficiency and productivity of defence use of M&S.

- **Improved quality:** The MSaaS Portal creates transparency about existing services and thus supports selecting the best possible service for a specific user requirement. In addition, reusing services and avoiding duplication of efforts will lead to higher-quality services.

Increase efficiency

- **Reduced Manpower requirements:** As a result of the automated processes (driven by cloud-based technologies and current deployment techniques), the personnel requirements on the end of the service consumer can be significantly lowered compared to the current situation. Since more services are available and spread around in a community of interest, more services can be accessed than before, some of these services are developed for e.g. the EXCON organization to be more efficient and support them to produce HICON/LOCON products.

- **Reduced reliance on SMEs and available expertise:** In the MSaaS concept, a lot of the required knowledge and expertise required to deploy simulations nowadays will be provided as a service. Therefore, reliance on SMEs can be significantly reduced.

- **Increased reuse opportunities:** MSaaS is about sharing the available M&S resources with the MSaaS community. By pooling these resources and providing them as a service to other stakeholders within the framework, the opportunities for reuse will be increased.

- **Reduced duplication of effort:** The MSaaS concept can reduce the duplication of effort by reusing common and consistent products and datasets as a result of pooling M&S products and data resources. Computing resources are pooled to serve multiple consumers concurrently. Different physical and virtual resources are dynamically assigned and reassigned according to consumer demand.

- **Reduced cost of ownership:** While the MSaaS concept removes the necessity for actual physical ownership of an M&S service, the cost of ownership will most likely be reduced.

- **Single point of access to M&S services**: The MSaaS framework provides a single point of access (e.g., through the MSaaS Portal) for the users. Each user is required to login into the MSaaS framework only once (single sign-on) and may access all resources permitted by his role.

- **Provisioning of M&S resources during runtime:** When running a federation of services, the system should allow to use new services or discard old ones, during runtime, without any disruption nor downtime in the system.

- **Leverage benefits of cloud computing:** MSaaS allows leveraging benefits of cloud computing, like scalability, resilience, etc.

3.9 Implementation Risks

Stakeholders that will implement the proposed concept into their organizations will also face risks and some major challenges. The following general (i.e. not defense-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, …)
- Dependency on network connections makes M&S applications vulnerable to network effects out of the control of an M&S user.
- Adapting existing M&S applications with a service interface or for hosting in the cloud may be complex and/or costly. Not everything fits in the cloud, especially if it hadn't been designed for the cloud.
- Non-localized control over consumed services creates a dependency and reliance on a service provider to fulfil their service level agreements and removes the possibility of manually modifying the service should the provider not do so.
- If a composed MSaaS service is validated for some use, updates to individual services may require re-validation. Mitigating this requires well defined service management and governance to allow service users to continue using validated services while newer updates go through the validation

process.

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

- Poor performance of network infrastructure available to military users, especially those deployed, may make access to and use of M&S services difficult or impossible.
- Dependency on remote infrastructure and services increases vulnerability in front-line/combat situations and makes local fallback options and backup systems necessary, thus cancelling out the major advantages of MSaaS for these situations.
- Adaptation of existing software is needed (e.g. replace internal weapon effects calculation of a simulation system with an interface to a service providing the same functionality). This may prove difficult or impossible in the case of COTS products. Note that it may be possible for some legacy/COTS products to act as an MSaaS by encapsulating it in a wrapper.
- In current distributed M&S applications, often significant tailoring of gateways etc. is required before use.
- Validation of specific services may be more difficult when they are more remote and internal operation is shielded to a large degree.
- Unwillingness of nations/companies to share resources.
- Unwillingness of companies to move to a pay-per-use model.
- Commercial constraints (e.g. procurement agencies don’t like pay-per-use model due to acquisition process constraints and limitations).
- Vendor (cloud provider) lock-in.