# Towards Multi-Level Security for NATO Collective Mission Training – a White Paper

*Björn Möller, Peter Karlsson - Pitch Technologies, Sweden*
*Stella Croom-Johnson, Dstl, UK*
*Tim Hartog, Wim Huiskamp, Cor Verkoelen - TNO, The Netherlands*
*Glyn Jones - Thales UK*
*Martin Normann Nielsen, FFI, Norway*
*Ingvar Ståhl, Swedish Armed Forces*

bjorn.moller@pitch.se, peter.karlsson@pitch.se
scjohnson1@mail.dstl.gov.uk
tim.hartog@tno.nl, wim.huiskamp@tno.nl, cor.verkoelen@tno.nl
Glyn.Jones@thalesgroup.com
Martin-N.Nielsen@ffi.no
ingvar.stahl@mil.se

Keywords:
Simulation, training, interoperability, NATO, security, Multi-Level Security

**ABSTRACT**: *Distributed simulation is rapidly becoming a necessity for collective mission training. With missions being joint and combined, we will never fight alone. Thus we need to train together, within and between nations. However, in any such scenario it is likely that some or all of the information may be classified at some level and need protection, be it scenarios, weapon and sensor capabilities or doctrines. In order for simulations to be interactive, one-way approaches such as data diodes will not work. Reclassification of systems using a "system high" approach has proven too complicated and expensive. This raises the need for true multi level security in collective mission training. This is indeed one of the big challenges in realizing the full potential of distributed simulation for defence purposes.*

*As part of the NATO RTO program a new modelling and simulation working group has been formed, MSG-080, to look at this topic. Initial members include Canada, Estonia, France, the Netherlands, Norway, Sweden, UK and the US. A kick-off meeting has taken place in October 2010 and a first round of knowledge exchange has taken place. An early conclusion is that most participating nations have similar requirements.*

*This paper summarizes the starting point for this group, including typical use cases where security solutions are needed, some basics about Multi-Level Security principles as well as a description of a few recent experiments carried out by some participants. Finally it describes some early considerations that were raised during the kick-off. Some examples are the need to obscure system capabilities, the need to support both simulation protocols and IT protocols (VoIP etc), the need for adequate performance and the need to get accreditation offices involved.*

## 1. Introduction

Modelling and simulation is an important technology that enables NATO to perform training, analysis, concept development as well as test and experimentation. Some particular benefits on the training side include saving time, money and even lives, when training unsafe scenarios. M&S also facilitates joint and combined training. Simulation based training is not necessarily constrained by range limits, thus facilitating larger exercises.

Development of distributed simulations is a complex process requiring extensive experience, knowledge and skill in order to design, develop and integrate systems into a federation that meets operational, functional, security and technical requirements. Federation architecture and design is the blueprint that forms the basis for federation-wide agreements on how to build a federation. Interoperability among distributed systems is however a multifaceted problem. It ranges from technical exchange of data via semantic issues dealing with a common understanding and use of information to mutually accepted security measures.

That latter aspect of information security is increasingly important as distributed simulation is rapidly becoming a necessity for collective mission training. With current-day missions being joint and combined, we will never fight alone. Thus we need to train together, within and between nations. However, in any such scenario it is likely that some or all of the information may be classified at some level and needs protection, be it scenarios, weapon and sensor capabilities or doctrines. Collective Mission Simulations need to satisfy accreditation requirements of more than one nation – this is a

lengthy and time-consuming process with a high cost overhead.

In order for simulations to be interactive, one-way approaches such as data diodes will not work. Reclassification of systems using a "system high" approach has proven too complicated and expensive. This raises the need for true multi level security in collective mission training. This is indeed one of the big challenges in realizing the full potential of distributed simulation for defence purposes.

NATOs Modelling and Simulation Group (NMSG) has formed a new working group, MSG-080, to investigate Security in Collective Mission Simulation. This paper summarizes the starting point for this group, including typical use cases where security solutions are needed, some basics about Multi-Level Security principles as well as a description of a few recent experiments carried out by some participants. Finally it describes some early considerations that were raised during the kick-off.

## 2. Scenarios and Use Cases

Security solutions may be required in many different types of collective mission training. This section summarizes some of the use cases that will serve as a basis for the studies of the MSG-080 group. These use cases have been contributed by several of the participating countries in MSG-080. It is worth noting thatuse cases from the different nations are very similar.

The purpose of the use-cases is to identify the problem space of security within these environments with respect to information security and ultimately to identify the way forward in possible solutions within this domain. This also implies that security issues that today exist within the physical space (e.g. physical protection of the perimeter wherein simulators are located) are out of scope of the use-cases.

For most use cases, training can be performed on different levels of the organizations or include multiple levels. E.g. for the first two use cases training and exercising can be performed from the technical to the tactical level, and for the third use case up to the strategic level. Note that the problem analysis should ultimately be described with respect to (1) preparation; (2) execution; (3) debriefing phases.

### 2.1 Status Quo: Training and exercise within one branch of the military services utilizing one training system

The training audience uses a training system specifically designed for one single purpose. Examples include counter improvised explosive device (C-IED) training systems, F-16 simulators and battalion/brigade level staff trainers. The training systems often reside on their own security domains and are often not designed to share information with other training systems or training systems of another vendor.

This use case describes to a great extent status quo. Information sharing needs are met for all stages of the exercises because information is only shared between participants on the same network and static trusted relationships are established a priori between systems. To realize the potential of distributed simulation, where existing training systems can be composed dynamically and provide new training opportunities, the two next use cases describe the direction in which we are moving and the information sharing needs in a multi level security environment.

### 2.2 Training and exercise within one branch of the military services utilizing several training systems and operational C2 systems

This use case is a live and virtual exercise. The training audience consists of a naval task force where the task group commander and staff use their regular C2 systems to be able to train as they fight. These systems are on security domain A. Subordinate units are staffed by a training audience using the embedded training capabilities of the operational systems onboard naval vessels (security domain B) and land based naval tactical trainers (security domain C). Exercise control (EXCON) is co-located with the land based naval tactical trainers. EXCON uses the local simulation capability to play opposing and neutral forces.

During the exercise the training audience subordinate to the task group commander and staff uses tactical data link information and voice communication to build a recognized air and maritime picture. This is based on shared ground truth data generated by the simulation capability on board the naval vessels and the land based naval tactical trainers. In addition they cooperate on engaging opposing forces generated by the simulation capability of EXCON. The task group commander and staff communicate with the subordinate units using voice and a military message handling system (MMHS).

The information exchanged across security domains B and C is simulation data for ground truth, tactical data link messages for perceived truth, voice data and MMHS messages. The information exchanged between security domains A and B and C is MMHS messages, voice and tactical data link messages.

### 2.3 Joint or combined arms training and exercising utilizing several training and operational C2 systems

This use-case is similar to the above but adds the security requirement of joint and combined

exercises. The example we will describe is that of Close Air Support (CAS) operations. This is a typical use-case for 'Security within collective Mission Simulations'.

The use case is split up in several individual sections. The first section describes the different (sub)goals of the Collective Mission Simulation. The mission goals determine which information is required and needs to be exchanged. They should always be considered when evaluating the security impact, the requirements and the solutions. The goals of a mission simulation can vary between different participants. The second section describes the participants. These vary depending on the required nations that should participate, the different disciplines of the defence organization and the required simulators that are needed to meet the mission goals. The third section determines the different interactions between the participating entities. These interactions take the mission goals into account; this should not describe all possible interactions that can occur between e.g. two simulators. It will only describe the interactions that are required between two simulators to meet the mission (sub)goal.

A typical Close Air Support (CAS) mission simulation includes a Forward Air Controller (FAC), a fighter aircraft (F16), and a target (Figure 1).

The overall mission goal is to get experience in international collective mission execution.

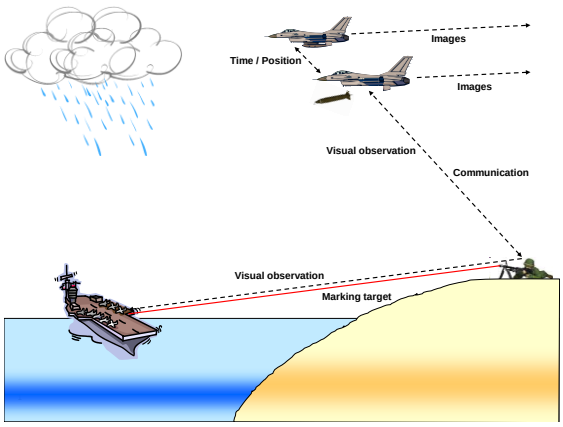


*Figure 1: Forward Air Controller use case*

In the CAS simulation case three nations participate: NLD is providing the fighter capability, USA is providing the FAC capability and UK is providing the target (including defence mechanism) capability.

The training goals can be divided into procedural training and mission rehearsal. The first sub-goal (SG-1) is to practice the procedure for the US FAC and NLD F16 in case of a close air support request, including e.g. "9-liner" communication. The second sub-goal (SG-2) is to rehearse an actual mission by the NLD F16's; this includes gathering intelligence information during flight and procedural maneuver training. The third sub-goal (SG-3) is also mission rehearsal, but then in an international context. This includes the request for close air support between nations, guidance of the fighters to their target and maneuver training during and after the actual weapon release.

Due to the sensitive information stored within the NLD F16 fighter simulators the simulators are classified as NLD-SECRET.

The FAC is provided by the US and classified as US-SECRET. There is a slight difference between the FAC simulator and the F16 simulator: the F16 contains classified information, the FAC does not by itself contain classified information; the voice information and procedures used are classified.

The third participating entity, the target of the CAS operation, is a UK navy ship simulator. This simulator contains sensitive information regarding the capabilities of the ship and is classified as UK-SECRET.

The fourth participating entity is a NATO command post that is used for the mission decision-making and which also receives the intelligence information provided by the NLD F16 simulator.

Furthermore a mission terrain database should be provided, however in our case we assume it is unclassified information.

For the information exchange it becomes clear that not only information is exchanged between different nations, but most likely also between different classifications.

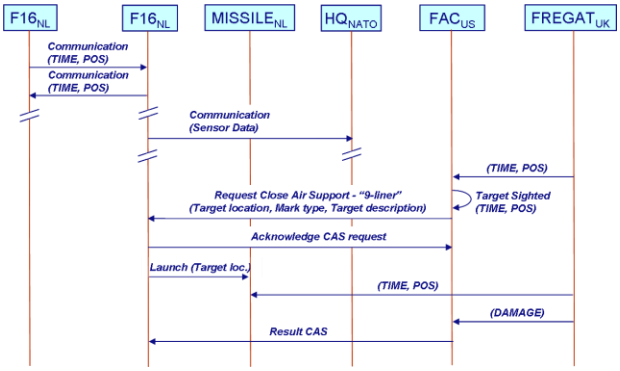


*Figure 2: Sequence diagram for CAS simulation*

Figure 2 shows a possible sequence diagram for the execution of the Collective Mission Simulation (CMS) in which all three sub-goals are performed. This sequence diagram shows the minimum of interactions needed between the simulators in order to reach the pre-defined mission (sub-) goals and this only serves as an example to clarify the security problem space. It is by no means meant to

present a complete and accurate information exchange between the different participating entities.

## 3. Risks and Threats

It must be noted that many of the risks and threats to information security in the CMS domain are identical to those seen in all other IT systems, for example hostile code or eavesdropping on wide-area network links. In these cases the obvious solution is to use existing tools and procedures, for example antivirus software, authentication, encryption, etc. As for most specialized applications, there are additional analysis methods and countermeasures that may need to be added to the standard tools. In addition to these general risks, all individuals need to be suitably cleared to see the outputs of the simulations. Even with controls in place to ensure the correct permissions are implemented and allocated, there remains a possibility of classified information being inferred from an aggregation of unclassified data.

### 3.1 Risks in General for Training Systems

As with any defence system, one of the major risks is unintended disclosure or leakage of information. In the training case and even more so in the mission rehearsal case, this could relate to the planned mission, the performance or capability of systems (sensor, weapon, etc) or the location of facilities. The leakage of task force composition, tactics and doctrines are other types of sensitive information.

In some case of hostile code intrusion or information obscuration there may even be a risk of negative training, if inappropriate or misleading information is provided.

On the analysis side a simulation system that has been manipulated may provide misleading or corrupt tactical and strategic analyses, possibly leading to suboptimal or even harmful decisions.

Hostile overload attacks (“Denial of Service”) may result in lost access to training facilities or analysis capabilities.

### 3.2 Information Disclosure in CMS

Currently simulators publish information without being able to control the destination of the information and without being able to diversify in the frequency with which the information is published to different recipients. Based on the interactions, the information classification and the actual information being exchanged, the problem space can be described as follows.

**Disclosure of classified information.** A first widely recognized problem is the disclosure of classified information through simulator interactions, e.g. sensor capabilities like the maximum resolution of the POD camera of the F16.

**Disclosure of information to (unknown) participants**. A second problem with current simulation technology is the lack of control regarding which recipient receives the published information. Because HLA uses a Publish-Subscribe mechanism any simulator can subscribe to the information of other simulators [1]. This may technically be needed in order to be able to execute the simulation. However, from a security perspective this is undesired because it diminishes the level of control an information owner has over the distribution of the simulator data.

E.g. in the CAS use case, SG-2 is focused on gathering intelligence data. This requires communication between the NLD F16 and the NATO Headquarters. For this sub-goal only the NATO HQ should be able to retrieve the sensor data (POD). In practice however every simulator can subscribe to this information and gain intelligence on the capabilities of the NLD F16s.

**Disclosure of new information through combining information.** Information that may need to be protected and is not disclosed explicitly could possibly still be derived from unprotected released data. For example, the actual speed of the NLD F16's may be derived from its frequent location updates. Due to the amount of data many possible combinations can occur, which makes it difficult to analyse which information could be gained by combining data.

## 4. Common Security Approaches

There are a number of approaches for handling data with different sensitivity and/or security classifications. This section provides an overview of them. They have different pros and cons and meet different requirements at different costs.

### 4.1 System High

In this approach all participating systems are reclassified to the same, highest level, for example “SECRET”. This means that all data and all systems are treated as if they were classified at the highest security level of any data in the simulation. This sometimes results in repeated reclassification of trainers, which may be cumbersome.

### 4.2 Multiple Single Levels of Security (MSL)

In this approach data and systems with different security classifications are processed in completely separated systems, for example one system for restricted information and one system for secret information as shown in Figure 3.

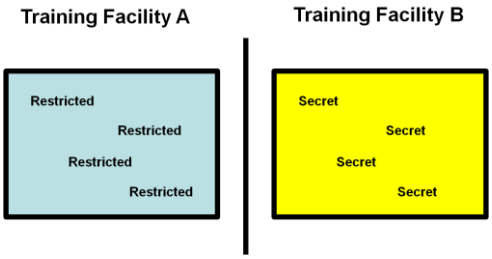


*Figure 3: Multiple Single Levels of Security*

Data may be transferred between domains using other means, for example by manually transferring information. In practice this often means that users need to operate several computers. This essentially moves the considerations from "how do computers process sensitive data" to "how do people process sensitive data".

### 4.3 Multiple Independent Levels of Security (MILS)

In this case data is also separated into different domains, depending on the classification. A one-way flow of information from lower to higher level is allowed, for example by using data diodes as shown in Figure 4. MILS is frequently confused with true Multi-Level Security.

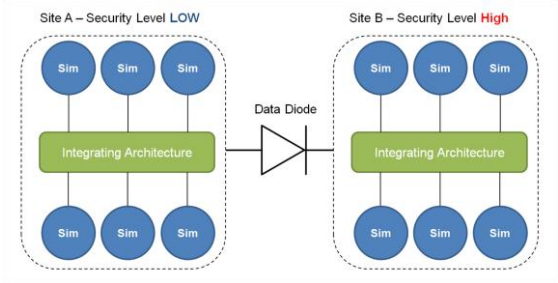


*Figure 4: Multiple Independent Levels of Security*

One major challenge with MILS and data diodes is that simulations need to be interactive while a data diode only allows for one way flow. As an example, a simulated aircraft in a lower security domain cannot see a simulated aircraft in a higher domain but it can indeed fire at it. The aircraft in the higher domain can indeed see the aircraft in the lower domain but it cannot fire at it. In spite of these issues, MILS is often used when only a limited set of information is required at the destination site, filtering of nearly all simulation data (e.g. UK-US 'JTEN' trials, where only the detonation information was required at the lower classification site).

### 4.4 Cross-Domain Solutions and Information Exchange Gateways

In this case a gateway is introduced, typically between two different security domains. A set of policies controls which data is allowed to flow between different domains as shown in Figure 5. In many cases one of the domains are considered to be "higher" than the other.

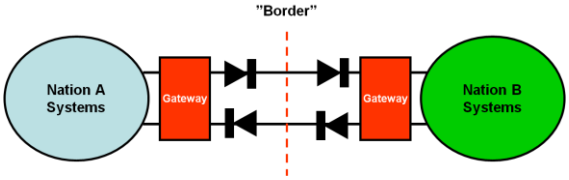


*Figure 5: Information Exchange Gateway*

There are obvious similarities to the work done with Information Exchange Gateways (IEGs) between for example NATO Command and Control systems. It should be noted that modelling and simulation has partly different requirements than Command and Control since for example effects, interactions and synchronization takes place in the information domain to a higher degree in M&S. Besides IEGs, cross domain solutions like labelling and release mechanisms can be applied to exchange information between different domains in a controlled manner [2] [3] [4].

### 4.5 Multi-Level Security

In Multi-Level Security (MLS) all information is stored in a trusted system that is trusted to contain sensitive data of various levels as shown in Figure 6.

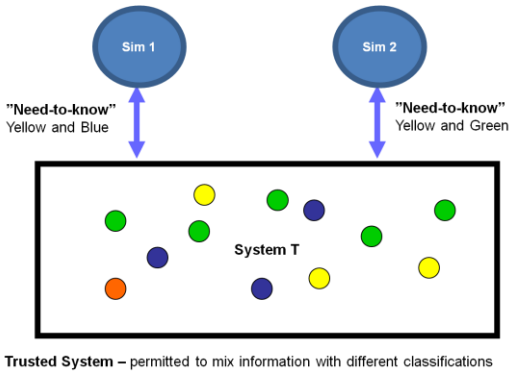


*Figure 6: True Multi Level Security*

The trusted system can release data to each system (or user) based on "need-to-know". The release mechanism, often referred to as Guard, may be based on the classification and information content.

### 4.6 Obscuring data

In some cases there may be a requirement to obscure data, for example by replacing one aircraft type with another (static obscuration) or the behaviour, for example the acceleration of a vehicle (dynamic obscuration). In particular the latter may require another behaviour model that provides an "unclassified" version of the behaviour. Whilst it is possible to sanitize data for transmission from a 'high classification' simulation to one of lower classification, there is no guarantee that the lower simulation can be repopulated with data that is

'good enough' leading to a danger of negative training.

For technical reasons there may also be a requirement to provide "dummy" values for data that has been removed, in order to prevent simulators that require these from crashing. If, for example, the nationality attribute of an aircraft is filtered out by a guard it may be useful to automatically insert a value representing "unknown" instead of transferring no data at all.

Another related approach is to use multi-resolution modelling and only provide aggregated information or information for selected entities to some participants.

In addition to the above obscuration of digital information it may also be necessary, during an exercise, to restrict the information exchange carried out through other channels, like voice communication.

### 4.7 General notes on pros and cons

Defining, verifying and maintaining proper security policies, in particular for guards, may not be trivial for many of the above solutions.

When most of the previously mentioned security approaches are introduced this will limit the information that can be seen and produced from some or all trainers. It is important to verify that the training is still both valuable and valid with these limitations.

Performance is another issue where it is necessary to verify that the introduction of security solutions don't have an adverse affect on the training goals.

Another challenge is to perform debriefing using systems with different classification levels. In this case it is necessary to prevent leakage of classified information. Some participants may even have training goals, that need to be debriefed, that may not be disclosed to other participants.

### 4.8 Configuration issues and workarounds

There are some particular configuration issues that occur when the same simulator needs to be used at different classification levels over time. This may be the case when one or more of the above approaches are used (for example MSL, MILS and System High).

A number of disc sets needs to be created and maintained at each participant site for each classification level. There are typically two variants of this approach:

- A set is created and maintained for each classification level.
    - Configuration control is a major headache.
    - This is also expensive in hardware and time.
- A master disk set is created and maintained; this is cloned and then configured for each required use. Typically one or more reconfigurable sets of disks are used, depending on the frequency of use at each security level.
    - This is cheaper in hardware but expensive in time as the disks need to be wiped after each use as required by the accreditor. This is time consuming and affects availability.

Often, a hybrid approach is adopted, as some items of networked equipment may not have user removable storage; examples may include networked projectors, real C2 equipment, etc. In these cases it might be appropriate to swap out the entire device (rather than just the data storage device) for one at the appropriate security level, or just to disconnect it and not use it during a connected event.

### 4.9 Removal of security requirements

Security measures must always be related to risks and threats and usually also to the benefits of a training event. Getting security accreditations and introducing the required measures will always take time and introduce some complexity. For some urgent missions this may be unacceptable, given the military threat or risk of losing strategic advantages. In this case high command levels may choose to reclassify the entire training event to become unclassified, or to mandate special security measures.

## 5. Early Experiments

In recognition of the need for more flexible security solutions, some NATO and Partnership for Peace (PfP) countries have already performed some early experiments. The design and experiences from these experiments are one of the sources that MSG-080 builds upon. There are also several other ongoing activities in participating nations that are being presented and discussed in the MSG-080 workshops.

### 5.1 Netherlands: Labelling and release

Within the Netherlands, a research program on information security defined a concept for the realization of a controlled information flow, including different topics within the information security work field. One of the mechanisms within this concept is the 'release mechanism'. This is based on determining a classification of information e.g. by interpretation of a label, and processing of a policy to decide whether the information may be released to the destination [2].

The first concept was based on the information release of documents within an electronic

environment. This concept was adjusted to identify whether the same concept could be used within other environments, not document based. The concept of labelling information within a simulation environment, using a policy, and decide whether the information may be published was realized using two simulators. The concept illustrates the possible technical solution of adjusting the information flows within a simulation environment, and the consequences of these adjustments for the 'execution' of a simulation.

The concept was able to interpret the information flow, determine the information 'value' and based on this value determine whether the information should be (1) altered; (2) deleted; (3) released unmodified. The concept also shows the limitation of the technical solutions, e.g. the lack of context of the simulation and the complexity of the filtering in case 'classified' information is not based on single information elements.

### 5.2 Sweden: MLS demonstrator

The Swedish defence has recently performed a Multi-Level Security study that included the development and demonstration of a prototype for a true MLS-solution that is compatible with the HLA standard. The initial study looks at four different use cases: national training, international training, simulation based acquisition and civil security. The first two use cases were prioritized.

A demonstrator was then developed and demonstrated. The scenario used for the demo was the international peace support "Terrateeka" scenario that was originally developed and demonstrated at I/ITSEC 2007 by the US and Sweden.

The demonstrator enables an HLA-compliant simulator to connect, without modification, to a trusted MLS-RTI. Policies ("need-to-know") can be developed and maintained both from a technical HLA-perspective and from a role-based user-perspective. The demonstrator supports several topologies to support various requirements for physical security of trusted data as well as different requirements for encryption of data links. The design also guarantees that the host of each simulator will only receive information based on the need-to-know of the simulator and/or operator.

## 6. NATO MSG-080

This section provides more details of the context and mission of MSG-080.

The North Atlantic Treaty Organisation (NATO) was established in 1949 to provide a stable Euro-Atlantic security environment based on growth of democracy and peaceful resolution of disputes. The NATO partnership also provides defence of its 28 members against external hostile intentions. The main objective of the NATO Research & Technology Organisation (RTO) is to conduct and promote co-operative research and information exchange to effectively use national defence research and technology to meet the military needs of the Alliance. This should enable NATO to maintain a technological lead.

The RTO consists of a number of Panels and Groups that organise and execute the research activities:

- Applied Vehicle Technology (AVT)
- Human Factors & Medicine (HFM)
- Information Systems Technology (IST)
- System Analysis & Studies (SAS)
- Systems Concepts & Integration (SCI)
- Sensors & Electronics Technology (SET)
- Modelling & Simulation Group (MSG)

The Mission of the NATO Modelling and Simulation (M&S) Group (NMSG) is to promote co-operation among Alliance bodies, NATO member nations and PfP nations to maximise the effective utilisation of M&S. The primary mission areas include M&S standardisation, education, and associated science and technology. The NMSG provides M&S expertise in support of the tasks and projects within the RTO and from other NATO organisations.

Given its mission regarding M&S and M&S related standards; it is no coincidence that NATO has acknowledged SISO as the Standards Development Organization for M&S. This was formalized in a Technical Cooperation Agreement (TCA) signed between NATO and SISO in July 2007 in Paris. The NMSG is also directly supporting SISO efforts, for example through C-BML, GM V&V, DSEEP and UCATT Study Groups. Many SISO committee members are also NMSG participants and the NMSG is ex-officio member of the SISO EXCOM.

### 6.1 MSG-080 Terms of Reference (ToR)

The overall objective of MSG-080 is to develop recommendations on how to create a collective mission simulation environment (procedures and processes, organisation and technology) that allows multiple security domains to participate. Sub objectives are:

- Initiate a Knowledge Network or Community of Interest (COI) for Federation Architecture, Security and Design
- Investigate through thematic workshops with subject matter experts:

    - Results so far including NATO and national regulations and directives, standards etc
    - Use-cases
    - Threats and vulnerabilities
    - Business requirements
    - Possible procedural, organisational and technical measures
- Develop solutions based on results from the investigation
- Evaluate, if necessary, one or more solution as an experiment
- Document and report experiences and results

Participating nations are expected to contribute with expert level members with knowledge and experience in designing federations of distributed simulations. To achieve the objectives it is necessary that the workshops are not only a forum for briefings, but a forum for discussion, networking and interaction.

### 6.2 Initial meetings

The overall plan contained a planning phase, four expert workshops and management group meetings. Summaries of discussions, suggested solutions and opportunities for future work are presented to the management group at the end of each workshop. The management group then decides on the priorities for the next workshop. The intention is that all material is stored in a NATO/PfP-wide shared workspace. Workshops are open for participation from the member nations. Key experts in security, federation architecture and related topics are identified by the management group prior to each workshop. Each workshop will focus on topics as prioritized by the management group.

The planning phase for MSG-080 took place between mid 2009 and early 2010. During this period an initial Programme of Work (POW) was developed and nations were requested to express their interest in participation through the NMSG. The first workshop (Oct 2010) focused on Security in CMS in general to scope current work and to provide a basis for the follow-on workshops. Different approaches and initiatives for Security in CMS will be presented by the member nations. Representatives from other domains will also be invited to share their experiences [3]. The expected result of the second workshop is a prioritized list of issues and an initial categorization and nomenclature for characterizing and classifying these issues. Initial members of MSG-080 include Canada, Estonia, France, the Netherlands, Norway, Sweden, UK and the US.

## 7. Early Conclusions and Road Ahead

The MSG-080 project has just started. The purpose of this paper is to spread the word, provide a common starting point and to summarize some existing knowledge and earlier experiments.

### 7.1 Some early conclusions

The early meetings have already provided a number of valuable discussions and conclusions. Here are some samples:

Security solutions may need to support many types of protocols: simulation protocols, IT-protocols (file sharing, etc) and VoIP and similar media protocols.

Security solutions must provide reasonable performance for most real-time or near-real-time simulations, in particular for tactical training.

The need for acceptance of new security solutions from accreditation offices may be a particular challenge. This needs to be addressed by involving accreditation specialists early on in the activities of MSG-080.

### 7.2 Road ahead

The road ahead for the project includes in-depth studies of selected use-cases in order to gain a better understanding of realistic requirements.

One of the following steps may include a practical experiment between participants. The scope and scenario of this remains to be decided based on the priorities of the group.

As the group has just kicked off its activity, now is the time for anyone who wants to provide input to his national representative or for NATO countries that would like to join MSG-080.

## References


[1] IEEE: "IEEE 1516, High Level Architecture (HLA)", www.ieee.org, March 2001.

[2] Security within Collective Mission Simulation Architectures, Cor Verkoelen, 09S-SIW-035

[3] IST-068 Study - XML in cross domain security solutions, RTO Report Pending

[4] B.J. te Paske, D. Boonstra, D.H. Hut, H.A. Schotanus, *Information Labeling – Cross-Domain Solutions*, Intercom Vereniging Officieren Verbindingsdienst, 38e volume nr. 2, june 2009.

## Author Biographies

**BJÖRN MÖLLER** is the vice president and co-founder of Pitch, the leading supplier of tools for HLA 1516 and HLA 1.3. He leads the strategic development of Pitch HLA products. He serves on several HLA standards and working groups and has a wide international contact network in simulation interoperability. He has twenty years of experience in high-tech R&D companies, with an international profile in areas such as modelling and simulation, artificial intelligence and Web-based collaboration. Björn Möller holds an MSc in computer science and technology after studies at Linköping University, Sweden, and Imperial College, London. He is currently serving as the vice chairman of the SISO HLA Evolved Product Support Group.

**STELLA CROOM-JOHNSON** is a Senior Analyst in the Analysis, Experimentation and Simulation Group in the UK Defence Science and Technology Laboratory (Dstl). She graduated from Southampton University (UK) in 1979 with an Honours degree in French, and from the Open University in 2006 with a First-Class Honours degree in IT and Computing. Before she joined Dstl in 2003 she worked as a computer scientist outside the defence industry. Since then she has worked on a variety of projects (including managing the DIAMOND Peace Support simulation model) and is the technical lead on a project looking at options for achieving a persistent Multi Level Security solution across standards and domains.

**TIM HARTOG** is working as an "information security" scientist at the Security department at TNO in the Netherlands. Tim graduated in 2005 at the Twente University of Technology, The Netherlands. During his work at TNO Tim has been involved in several research projects covering topics like Trusted Operating Systems, Cross Domain Solutions and Trusted Computing.

**WIM HUISKAMP** is Chief Scientist Modelling, Simulation and Gaming in the M&S department at TNO Defence, Security and Safety in the Netherlands. He received a M.Sc. degree in Electrical Engineering from Twente University of Technology, The Netherlands. His research areas include system architecture, distributed real-time simulation and C2-Simulation interoperability problems. Wim acted as project lead for several national and international simulation (interoperability) projects and he leads TNO's research programme on Live, Virtual and Constructive Simulation, which is carried out on behalf of the Dutch MOD. Wim is a member of the NATO Modelling and Simulation Group (NMSG) and acted as member and chairman in several NMSG Technical Working groups. He is currently Chairman of the NMSG M&S Standards Subgroup (MS3) and is the liaison of the NMSG to the Simulation Interoperability Standards Organization SISO.

**GLYN JONES** is a Technical Manager with responsibility for Information Security research at Thales Research & Technology (UK) Ltd. He graduated from Durham University in 1978 with a degree in Applied Physics and Electronics. Glyn has a background in telecommunications and military communications systems and has been working in Information Security research since 1999. Subjects of particular interest are application layer security for control of access to data and cyber security.

**PETER KARLSSON** is a senior project manager at Pitch. He has ten years of experience in software engineering, including working with Role Based Access security policies for the CERN particle accelerator complex and several years working with interoperability in modelling and simulation in Swedish and NATO projects. Peter Karlsson holds an MSc in computer science and engineering from Linköping University, Sweden.

**MARTIN NORMANN NIELSEN** is a Scientist at FFI (Norwegian Defence Research Establishment) where he is working with distributed simulation technologies. He completed his M. Sc. in Computer Science at the University of Oslo in 2006. His research interests include modelling and simulation, computer security, wireless communication systems and command and control systems.

**INGVAR STÅHL** is working for the Swedish Armed Forces and is responsible for Concept Development and Experimentation in the area of Secure Effective and Efficient Information Management, SEEIM. He is the former head of Military Information Security Service and holds an MSc in Electrical Engineering from the University of Technology in Lund. He is currently liaison to NATO Capability Panel 4 and to NATO Information Management Advisory Group.

**COR VERKOELEN** is an Information security scientist who graduated in 2000 in the area of 'Telecommunication and Informatics' at the Netherlands. Subsequently he joined TNO Defence and Security specializing in the area of information security. He started his career by doing research on penetration testing and defences against digital attacks by following new emerging technologies. Later he included the architectural and business side of information security and became an all-round security scientist. Since 2006 Mr. Verkoelen is involved in several research projects (technical as well as at organizational level) that cover the problems around the interconnection of information systems. In line with this background he started the research on possible solutions within the simulation environment which he feels copes with the same problems as other information systems seen from a security point of view.

*This paper has been reviewed and endorsed by NATO RTO-NMSG for presentation in SISO.*