Security in NATO Collective Mission Training - Problem Analysis and Solutions

Björn Möller - Pitch Technologies, Sweden
Stella Croom-Johnson, Dstl, UK
Tim Hartog, Wim Huiskamp, Cor Verkoelen - TNO, The Netherlands
Glyn Jones - Thales UK
Matthew Bennett, BAE Systems, UK

bjorn.moller@pitch.se
scjohnson1@mail.dstl.gov.uk
tim.hartog@tno.nl, wim.huiskamp@tno.nl, cor.verkoelen@tno.nl
Glyn.Jones@thalesgroup.com
Matt.Bennett@baesystems.com

Keywords:
Simulation, training, NATO, security, requirements, DSEEP, information exchange

ABSTRACT: *We never fight alone, so we should train together! With missions being joint and combined, we also need to train that way. Given limited budgets and available resources, distributed simulation is rapidly becoming a necessity for collective mission training. However, due to the characteristics of mission simulations the protection of classified information (e.g. scenarios, weapon and sensor capabilities or doctrines) becomes a serious security challenge. As part of the NATO RTO program a new modelling and simulation working group has been formed in 2010, MSG-080, to look at this topic. Members include Sweden, UK, Estonia, the Netherlands, Norway and the USA.*

This paper describes in detail the security challenges which we face and analyses the technical characteristics of simulators in relation to the information that needs to be protected. Based on these findings the effectiveness of different identified security solutions to the security challenges at hand can be further explored. Security solutions which are considered include data diodes, cross domain solutions (labelling and release mechanisms) and Multi-Level Security. The challenge is to prevent information leakage without compromising the primary training objectives. By approaching the stated security challenges in an integral manner we aim to find solutions which can provide adequate performance and which are also acceptable for accreditation authorities.

1. Introduction

Modeling and simulation is an important technology that enables NATO to perform training, analysis, and 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. Interoperability among distributed systems is however a multifaceted problem. It ranges from technical exchange of data through 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 – often more than one level - and needs protection, whether it be related to scenarios, weapon and sensor capabilities or doctrines.

Collective Mission Simulations (CMS) 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 defense purposes.

NATO's Modeling and Simulation Group (NMSG) formed a working group in Q4 2010, named MSG-080, to investigate Security in Collective Mission Simulation. This paper summarizes the findings of this group up to now, elaborating on the previous paper "Towards Multi Level Security for NATO Collective Mission Training" [1]. This paper explores the characteristics of CMS and provides a break-down of the simulator and simulation to gain a better understanding of the information security challenges within CMS. Furthermore it provides an integral view on security within CMS.

2. Characteristics of CMS

CMS has some very different characteristics when compared to 'real-world live missions' and other domains (e.g. office automation). These characteristics have a direct impact on the requirements regarding security solutions.

2.1 Differences between M&S and Live Mission Training

When compared to Live Mission Training CMS has several distinct characteristics. These characteristics have an impact on the security issues which are present within CMS.

- Information value

  One of the main differences between CMS and other domains is that simulators need 'exact' information in order to function. Since simulators are often equipped with operational software and models all their output is 'exact'; we call that "ground truth". That information gives direct insight into the simulator's capabilities. When we compare this to the 'real-world' situation the information which can be gained there is only 'perceived' truth, depends on the participant's ability to perceive events and the accuracy with which those events can be perceived.

- Visibility / Radius

  In addition to the value of the received information the exposure radius of information is larger in CMS. Ground truth data includes detailed interactions of sensors and weapon systems and is potentially visible to all participating entities in the CMS. In the 'real-world' such information is typically only visible for entities in the immediate vicinity of such events.

- Sample size

  CMS offers the possibility to execute the same operation(s) over and over again. This may be under identical or slightly different circumstances (e.g. weather conditions). This allows for analysis of 'big sample size' and thus deduction of information that is otherwise hard to obtain.

There are also particular M&S considerations when security measures are taken:

- Is the training still valid?

  Security approaches often work by limiting 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.

- Is the performance sufficient?

  Performance is another issue where it is necessary to verify that the introduction of security solutions does not have an adverse effect on the training goals.

- Can relevant debriefing be provided?

  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, which need to be debriefed, but which may not be disclosed to other participants.

2.2 Security concerns within CMS

There are several security concerns within the execution of a CMS, which can be intensified by the afore-mentioned distinctive characteristics of CMS.

To achieve the objectives of many Joint Collective Training exercises, large amounts of information have to be shared between participating simulations, but at the same time that information – which may be classified – needs to be protected. This needs a balancing act between the risks arising from the leakage of data versus the risks of providing suboptimal training.

The former includes:

- Unintended disclosure or leakage of:
  - Planned mission
  - System performance and capability
  - Task force composition
  - Tactics and doctrines
  - Facilities
- Unwanted, misleading or corrupt tactical and strategical analyses.
- Lost access to training facilities or analysis capabilities.

The risks arising from suboptimal pre-deployment training include:

- Lack of familiarity with:
  - Planned mission
  - System performance and capabilities
  - Task force composition
  - Tactics and doctrines
  - Facilities
- Negative learning (e.g. Sensor capabilities)

These issues can manifest themselves in different ways, and may not be immediately apparent, but in either case could lead to a less effective mission and higher casualty numbers once trainees are deployed to theatre.

Not all security concerns are considered in scope for MSG-080.

- Information leakage of confidential information in the simulation over RTI/HLA is considered in scope.
- Information leakage due to physical access, viruses/malware, human-to-human communication as well as information leakage due to subsequent transmission to a third party is considered out of scope. These concerns are not specific to the CMS domain and are addressed by general information security measures.

Information leakage can occur on three levels

- Direct external leakage of classified information
- The transmission of prohibited data from one controlled network to another which can be caused deliberately or arise accidentally, but needs to be protected against.
- Combined information, for example:
  - An accumulation of unclassified data can, in sufficient quantities, unintentionally reveal classified information.
  - Meta information
    Information can be derived from the examination of events and actions within a scenario. A sequence of actions within a simulation can reveal data at a higher classification level than is acceptable

2.3 Security requirements and impact on CMS

There are several types of security mechanisms as well as ways to deploy them. Their ability typically includes:

- The ability to filter on information level (what do you want to share and what not)
- The ability to filter on communication level (what do you want to share with whom)

There are several factors for which the security mechanisms need to be controlled in order to minimize the impact on the execution of CMS, for example

- Timing (real-time)
- Impact on training realism
- Possibility for accreditation
- Feasibility of the solution

Security solutions and processes will inevitably have an impact on M&S applications. The issues identified are described in this section.

Security solutions often impose latency and reduce available bandwidth. Interactive simulations that have man-in-the-loop operators need low latency and high bandwidth data exchange. This may add performance requirements to M&S middleware.

Requirements for simulation models can also be affected. Simulation models may have to be more easily tailored to address different classification levels. For example parameters and settings should be configurable. This can however have an impact on the credibility of the simulation if the new parameters are less realistic. It could also be possible to alter information before sharing with other simulators, making it seem to operators that the systems behave in unexpected ways and thus it can compromise the credibility of the exercise. E.g. the entity ID and visual model of the F-117 (Stealth) may be changed into that of an F-16. However, the F-16 will then show a strange behaviour in the eyes of an observer by flying slower and at low altitudes near air-defence installations.

Modern simulators more often run ‘operational software’ as part of the simulator. This development is the result of the desire to keep simulators up-to-date with the actual platforms (e.g. F16 flight management software) and at the same time reduce maintenance costs for the simulator. This software is usually highly classified. Modifications to this software to address classification and M&S concerns are difficult or impossible. A second consequence is that after updating the operational software package a re-accreditation may be needed. That process can take 18 months, whereas flight-management software updates may have cycle times of 6 months. Security requirements impact the simulation federation development process e.g. when using DSEEP. This

may also mean that security accreditation has to be partially repeated when the same simulation is re-used with different players and or different scenarios.

Simulation infrastructures are often reused in differently classified exercises to reduce costs. In many cases, data may not cross the border between two different exercises. Alternatively, there may be the need to run an exercise and a during action review (DAR) session in parallel on the same infrastructure, with the DAR having a different classification.

To some extent the exchange of classified data can be reduced by designing the training and the scenario to minimise the need for this. However, in some cases the classified data is essential to the success of the training, making some exchange of this data inevitable. An important consideration here is whether the data is sufficiently important to the objectives of the exercise to warrant the measures that need to be put in place to obtain accreditation. The impact of those measures on factors such as latency, bandwidth etc must also be taken into account.

2.4 Accreditation

Accreditation of security solutions has an impact on development schedules. The process of implementing security solutions and obtaining accreditation is complex and takes significant amounts of time and resources. This impacts the ability of nations and NATO to address the need for quick turnaround times for training and mission rehearsal using M&S.

Information which the accreditors may require before approving an event include:

- Purpose of the simulation
- Network configuration
- Classification levels involved
- Risks/threats with potential consequences
- Evidence of how risks can be managed

In all cases accreditors will be looking for evidence that the security risks associated with data exchange between networks is managed, and has been reduced to an acceptable level.

3. Analysis of Simulation and Simulators

As earlier described, information in CMS can be sensitive or classified information. A better understanding of the types of information within a CMS is required to be able to come to a proper security solution. This section provides a framework to better understand:

(1) The kind of information in a typical defence simulation.

(2) In what way this information can be sensitive.

This will be described from two perspectives. The first perspective is from that of a federation with multiple simulators to execute a shared scenario. The second perspective focuses on information within a particular simulator. Note that the example used here focusses on HLA, but similar considerations apply when using other interoperability solutions.

3.1 Information within a Federation

The federation consists of a number of simulations, known as HLA federates [2], that exchange data through a HLA Runtime Infrastructure (RTI). This is shown in Figure 1.

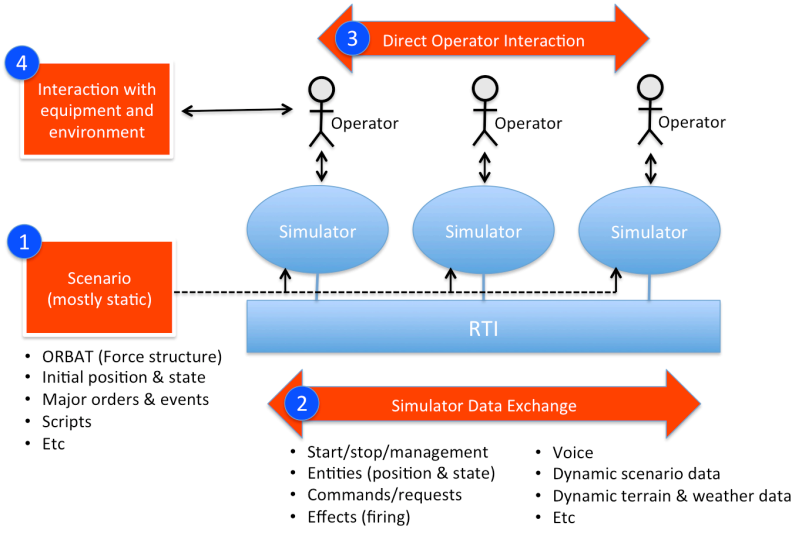

Figure 1 – Information in a federation.

The shared information in the federation can be divided in four categories.

1. Scenario

   Describes the involved forces and how they are structured (positions, types, nationalities, etc), also known as Order of Battle (ORBAT). This information is mostly static. The scenario may be sensitive since it contains information about force structures, planned operations as well as tactics and doctrines. The information can be particularly sensitive in the case of mission preparation or mission rehearsal training.

2. Data exchange over the RTI

   The actual data exchanged is highly dynamic. It contains management data (start/stop), position and state of participating entities, commands, weapon engagements and effects, etc. This information may be sensitive since it reveals tactics and doctrines, weapon and sensor capabilities and many other aspects of the trained operation.

3. Direct operator interaction

   The interaction between operators may take place directly through voice, gestures, radio, phones and other communication means. The exchanged information may be sensitive. This kind of information exchange falls outside the MSG-080 problem-scope.

4. Equipment interaction

   There may also be interaction with real equipment and the physical training environment. The procedures and purpose of these interactions may be sensitive. This also falls outside the MSG-080 problem-scope.

3.2 Information within a simulator

A simulator can be seen as a combination of static information (the scenario and environment), models for the behaviour of the simulator components (mainly static), operator input and the actual state of the simulation (highly dynamic). This is shown in **Error! Reference source not found.**.

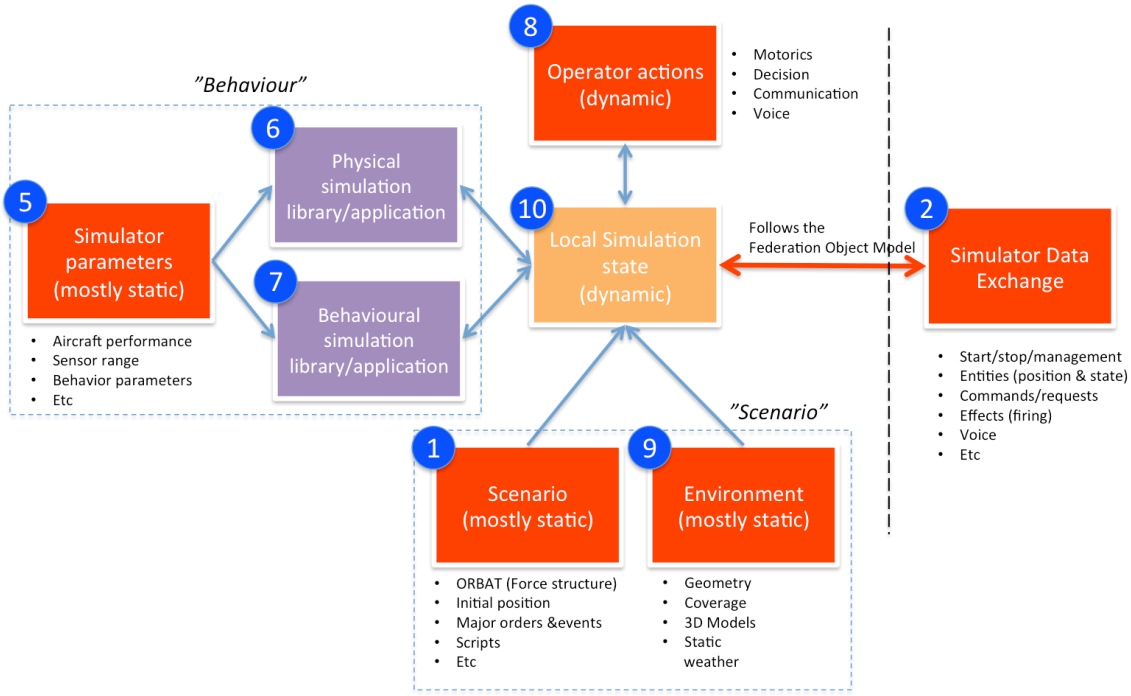

Figure 2 - Information in a simulator.

The information in the simulation is the same as bullets 1 (scenario) and 2 (simulator data exchange) above. There are also some additional types of information:

5. Simulator parameters

   This may be the characteristics and performance of an aircraft (sometimes called the "data package"), weapons performance or sensor parameters. This may obviously be highly sensitive information, in particular for new systems where the public knowledge is very limited. These parameters are usually quite easy to replace with less sensitive values when executing on joint or combined scenarios.

6. Physical simulation libraries/applications

   This is software that simulates the physical characteristics of an entity like a platform or a weapon. This is sensitive in a similar way to simulation parameters but may reveal even more details of the actual performance of a system.

7. Behavioural simulation libraries/applications

   This is software that simulates behaviour, tactics, strategies and doctrine. These may of course all be very sensitive.

8. Operator actions and interactions

   These interactions with the simulator can cover everything from movements to decisions and communication. All of this may be sensitive.

9. Environment data

   This is mostly static data. It contains general terrain geometry and terrain coverage as well as cultural feature and possibly classified defence features (fortifications etc). There is a multitude of formats for terrain data, including the CDB, OpenFlight and OpenSceneGraph. The terrain data may be delivered as files, databases or by streaming. Today most simulators have their own terrain data, but in the future a shared terrain data service will become more common. Three-dimensional models of buildings, vehicles, weapons and more are also needed. Some parts of the weather may also be described here. Terrain data may be sensitive since it may describe classified areas and facilities or because it has a higher resolution and accuracy than commonly available terrain data. There are frequently also IPR issues with terrain data.

10. Local simulation state.

    The state is a result of the other information as described above. It is sensitive since it may be used to deduce the previously mentioned types of information.

Looking back at some of the potential technical security solutions mentioned in the previous SIW paper [1], such as Cross Domain Solutions and MLS, we can see that these solutions require some sort of classification/labelling of the information in order to decide if the information can be shared. The question is to what extent it is possible to classify/label the static and dynamic type of information.

4. Integral View on Security in CMS

When addressing the topic of information security within the Collective Mission Simulations environment it becomes clear that technical information security measures alone will not be sufficient to solve the information security challenges at hand [3], [4]. In order to realize an effective solution we can divide possible security measures into three different categories; these categories being measures taken at (1) Organisational level; (2) Process level; and (3) Technical level.

These three categories show similarities with the development of a simulation (e.g. within DSEEP). During first three DSEEP steps of developing a federation, the goals and subgoals, the conceptual model and the federates are determined. This includes allocation of responsibilities to different federates, i.e. who simulates what. It then becomes clear what information needs to be exchanged during the simulation and it can be determined whether (at this stage) it is acceptable to exchange it.

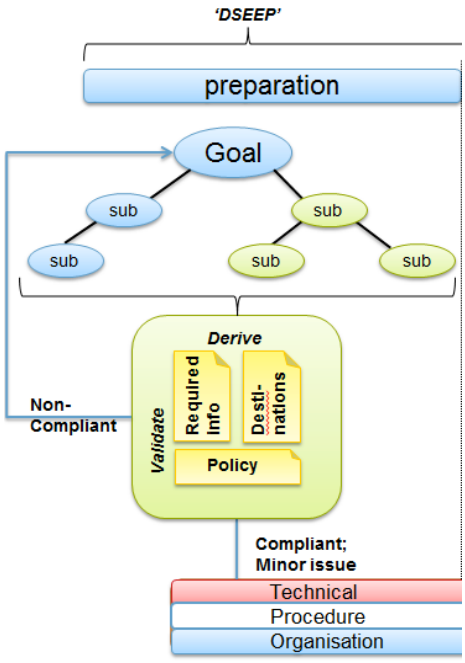

Figure 3 Development of federation

This decision depends on the different policies that apply for the organization of the information owner and the information itself. This is the first category: the measures at the organizational level. In short, the measures that can be taken at the organizational level must include the security requirements (and to validate the compliance with policies and requirements) based on the information that is required for the execution of the simulation.

The second category comprises the measures at the process level. At the process level the different CMS goals are defined. At this point the exact required information should become clear. Therefore the impact on the required information exchange also becomes clearer. A second validation of compliance with policies and (national) security requirements should be performed. During this validation, and possible conflicts, the impact on the CMS goals should be described. After the validation a 'risk assessment' can be performed to decide whether (1) no conflicts are found, and all information required can be exchanged without further security measures; (2) conflicts are found and technical measures should be put in place to overcome these conflicts (e.g. filtering the information); (3) conflicts are found for which no technical measures can be implemented (e.g. because there are no measures with enough assurance due to the high classification of the required information). In the latter case the impact of not exchanging the information on the CMS goals should be described. The organization itself should then decide what to do with these CMS goals.

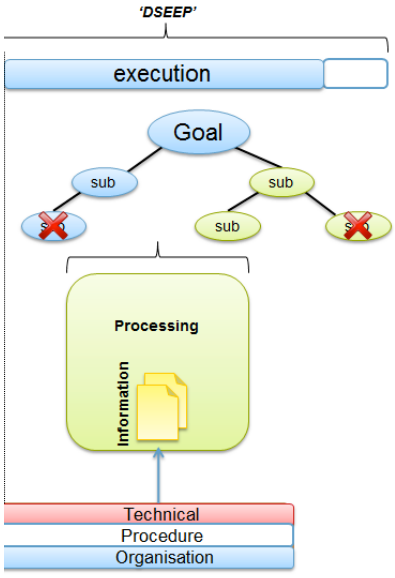

Figure 4 Execution of federation

The third category comprises the measures at the technical level. A previous paper by MSG-080 [1] already described several possible technical security measures. These security measures should limit the risk of information leakage. Which kind of security measure should be implemented depends on several factors, e.g. on the classification of the information. The impact of a security measure should be described. This impact description should be available at both the process and organizational levels to determine the impact on the simulation, and simulation goals.

The three categories and the logical flow for the development and execution of a federation are shown in Figure 3 and 4.

5. NATO MSG-080

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
  - 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

The MSG-080 activity was started in Q4 of 2010 and will finish at the end of 2012. The findings will be presented in a final report. A follow-on activity is considered that will experiment with some of the proposed new technologies within the framework of other NATO distributed simulation events.

6. Early Conclusions and Road Ahead

6.1 Early conclusions

Security in CMS is not a new challenge, but with increasing amounts of joint collective training being

carried out its profile has been raised significantly in recent years. It would be counter-productive to expect a 'one size fits all' solution in the near future, but this study has looked at a number of steps that could be taken to improve the situation in the short term. The taskgroup has reached a better understanding of why, where and how M&S differs from Live and other domains w.r.t. security.
There is also a much better understanding of how security impacts CMS.

MSG-080 has been working on improving the conceptual model of how to classify and structure security related issues in M&S. This is a starting point for evaluating technical solutions.

The conceptual model is also a possible starting point for integrating security issues in the development process and may lead to a DSEEP 'overlay' regarding security aspects.

6.2 Road ahead

In addition to the previously mentioned experimentation plans, the MSG-080 team is also preparing a SISO Study Group on this topic. The objective is to encourage the wider simulation community to contribute to this investigation. Security challenges for distributed simulations are obviously not limited to the military domain. Many businesses and organizations are facing similar issues when there is a need to cooperate while still having to protect their business intelligence or their intellectual property.

The objective of the SISO study group is to ensure that common standards are developed for technical solutions. These standards should be open and should not result in conflicts with existing simulation interoperability standards like HLA and development processes like DSEEP.

References

[1] B. Möller, et all, *Towards Multi-Level Security for NATO Collective Mission Training – a White Paper*, 11S-SIW-069, 2011

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

[3] C. Verkoelen, et all, *Security within Collective Mission Simulation Architectures*, 09S-SIW-035, 2010

[4] B.J. te Paske, et all, *Information Labelling – Cross-Domain Solutions*, Intercom Vereniging Officieren Verbindingsdienst, 38th volume, nr. 2, June 2009

Acknowledgements

The authors would like to acknowledge the contributions of the other members of the MSG-080 Taskgroup to the ideas and results presented in this paper.

Author Biographies

BJÖRN MÖLLER is the vice president and co-founder of Pitch Technologies, the leading supplier of tools for HLA Evolved, 1516-2000 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. He is currently serving as the vice chairman of the SISO HLA Evolved Product Support Group.

STELLA CROOM-JOHNSON is a Principal Analyst in the Analysis, Experimentation and Simulation Group in the UK Defence Science and Technology Laboratory (Dstl). 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.

WIM HUISKAMP is Chief Scientist Modelling, Simulation and Gaming in the M&S department at TNO Defence, Security and Safety in the Netherlands. Wim 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 co-chair of MSG-080, Chairman of the NMSG M&S Standards Subgroup (MS3) and he is the liaison of the NMSG to the Simulation Interoperability Standards Organization SISO.

COR VERKOELEN is an Information security scientist at TNO Defence and 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 and he started research on possible security solutions within the simulation environment.

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 various research projects covering the problems around interconnection of information systems in Military domains. Research topics of interest are Cross Domain Solutions, IEG, Trusted Operating Systems and Trusted Computing.

MATTHEW BENNETT works for the Future Capability team within BAE Systems Military Air and Information business. Matthew graduated in 2004 at Loughborough University in the UK. In his time at BAE Systems he has worked on the embedded training systems within the Hawk family of Advanced Jet Training aircraft. Subsequently he became a Research Engineer, addressing challenges with beyond line of sight communications technology including security for embedded synthetic training systems within front line aircraft.

GLYN JONES is a Technical Manager with responsibility for Information Security research at Thales UK Research & Technology. Glyn has a background in telecommunications research and military communications systems and has been working in Information Security research since 1999. Subjects of particular interest are cyber security and application layer security for control of access to data.