Tanks Don't Tweet: Implementing Information Warfare Simulation

James Kearse
Thales UK Limited
Crawley, United Kingdom
james.kearse@uk.thalesgroup.com

Dr Keith Ford
Thales UK Limited
Crawley, United Kingdom
keith.ford@uk.thalesgroup.com

ABSTRACT

Information effects such as psychological operations, computer network operations and the use of media as an influence tool are of increasing importance to military users. However, current modelling and simulation environments have a limited representation of these aspects, having evolved to represent the physical environment and physical warfare effects. Human role players are often used in exercises to simulate information effects but this is expensive and does not consistently provide an accurate and detailed representation of the information environment. As a result, commanders are not currently able to deploy information warfare effects using currently available training systems. Future simulations must be able to provide improved representations of operational environments including information effects such as disrupting communications or networks, spoofing messages and the use of social media for information operations purposes.

Under funding from the United Kingdom Ministry of Defence, Defence Science and Technology Laboratory (Dstl), Thales UK have undertaken research as part of the Synthetic Environment (SE) Tower of Excellence[1] into the implementation of information warfare within simulation. In order to investigate information warfare effects, the team developed a test-bed using off-the-shelf components. The test-bed has been used to investigate a series of use cases based around information operations and media operations scenarios.

As well as discussing the experimentation and the practical consequences for integrating of information warfare into Simulation and SEs, the paper considers the implementation of Information Warfare in the context of MSaaS. The MSaaS concept, as developed within NATO Modelling and Simulation Group (NATO MSG) 136, promotes the delivery of simulation capability as services with well-defined functionality and interfaces. The results from the research shows that this approach is desirable when simulating information warfare effects as it enables physical, network, information and cognitive effects to be managed independently in an extensible open framework. Recommendations for the practical integration of information warfare services into current simulations are also provided.

ABOUT THE AUTHORS

Dr Keith Ford has worked in the simulation industry for over 35 years. During this time, he has worked on display systems, control loading, motion systems (for which he obtained his doctorate) and for the last 18 years in the field of synthetic environments. Keith is currently the Research and Technology (R&T) Manager at Thales Training & Simulation (UK) and is responsible for all internally and externally funded R&T projects. He is currently the technical lead for Dstl funded projects that are researching the issues for providing Modelling & Simulation as a Service and Information Warfare.

James Kearse started his career at QinetiQ in 2004 where he worked on a range of land and air based simulation and training research programmes. These included the UK Mission Training through Distributed Simulation Capability Concept Demonstrator (MTDS CCD), and the Training for Combat Readiness research programme. In 2010 he moved to Thales UK where he has supported a number of UK training services and the Dstl SE Tower research programme.

[1] The research underpinning this paper was conducted within Technical Column 2 of the SE Tower, under the Synthetic Composition and Representation of Natural and Physical Environments (SCORE) contract.

Tanks Don't Tweet: Implementing Information Warfare Simulation

James Kearse
Thales UK Limited
Crawley, United Kingdom
James.kearse@uk.thalesgroup.com

Dr Keith Ford
Thales UK Limited
Crawley, United Kingdom
Keith.ford@uk.thalesgroup.com

BACKGROUND

Introduction

The use of information in warfare is nothing new. Indeed, Sun Tzu remarked that *'supreme excellence consists in breaking the enemy's resistance without fighting'* [1], illustrating that information was a powerful component of conflict even in 500 BC. While the use of information has remained a constant within military operations, the ubiquity of information technology has enabled military commanders to use information in new ways. Recent geopolitical events have illustrated that information effects can be implemented alongside traditional military effects; giving rise to terms such as hybrid warfare[2] [2] and information confrontation[3] [3]. For the purposes of this paper, and in lieu of a single agreed definition, the following definition of information warfare is used; "*The process of protecting one's own sources of battlefield information and, at the same time, seeking to deny, degrade, corrupt, or destroy the enemy's sources of battlefield information*" [4]. Within information warfare, the operations undertaken can be as diverse as Computer Network Operations (CNO), Psychological Operations (PSYOPS) or Media Operations (Media Ops) or a combination of all of these activities.

United Kingdom (UK) military doctrine is based around the principle of Joint Action [5] where information effects are employed alongside and in concert with physical or kinetic effects. Joint Action also includes the concept of Full Spectrum Targeting where a holistic approach to applying effects is taken and the most appropriate physical or information effect is selected by the commander. Military commanders increasingly possess the option to employ both physical and information effects against their targets in a coordinated and integrated fashion. Furthermore, these targets may be increasingly non-military in nature and could include physical infrastructure, computer networks, broadcast media, social media and the attitudes and opinions of an audience within the battlespace.

The Modelling and Simulation Problem Space

While information warfare is of increasing importance, and becoming more integrated into conventional military activity, Modelling and Simulation (M&S) systems currently have a limited ability to represent both the information environment and information effects. This is unsurprising; the genesis of our M&S systems and their underpinning standards was during the Cold War. At this time, physical engagement-based effects designed to damage or degrade adversaries were prioritised, with physical terrain providing the basis for the operating environment and a singular 'Red Force' populating the world. These systems were well suited to their task, but their legacy is that the information environment is currently only represented in part within simulation, if at all.

The operating environment is increasingly multi-dimensional in nature, with military commanders needing to understand, manoeuvre and apply effects within several overlapping domains. These include the need to attack, defend and exploit information held on computer networks, understand and influence the attitudes and opinions of both individuals and groups, and understand, target or develop critical civilian-owned infrastructure such as sites used for power generation.

Instead of Blue (friendly) and Red (enemy) forces, the battlespace now includes a large population of diverse actors, audiences and adversaries. These include both influential individuals and groups. Groups may range in size from

[2] Hybrid warfare refers to a blend of traditional military activities with information activities.

[3] Actions short of war but which use information to achieve an advantage over a competitor or adversary.

tens to thousands of people and may include entities as diverse as Non Governmental Organisations (NGOs), street gangs, organised crime, religious groups, tribes and militias. Allegiances may fluctuate between these groups; and their attitudes and opinions towards key topics will become elements that will need to be represented within modeling and simulation environments. While the operating environment has become increasingly complex, our M&S environments have not kept pace with this complexity.

The 'as is' and 'to be' situation in terms of the representation of information warfare within M&S systems is highlighted below in Figure 1.

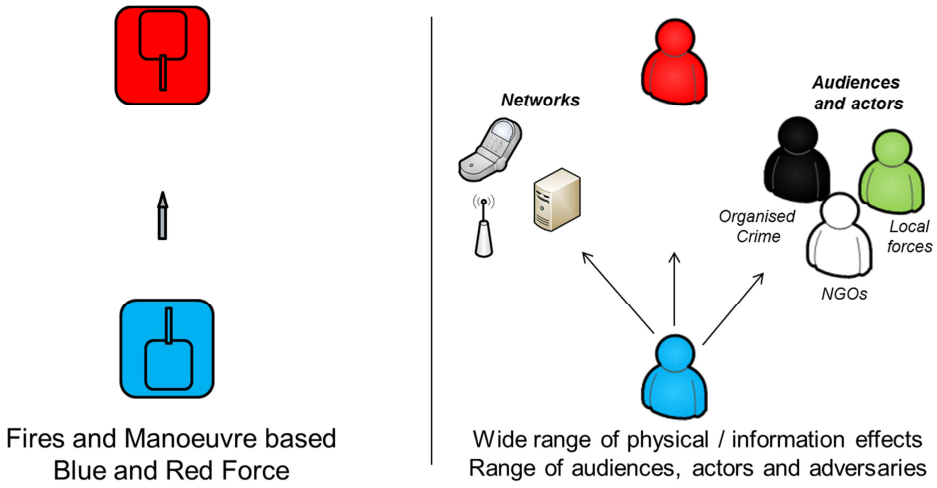

Figure 1. Representation of effects and audiences within modelling and simulation system; the 'as is' is on the left, with the 'to be' on the right.

The current approach for representing the information environment within M&S events relies upon human role players to input the relevant expertise. However, this is a manpower-intensive activity and may result in information warfare elements being inconsistently represented, not repeatable or not fully integrated with conventional elements. The consequence of not replicating these aspects effectively is that our warfighters will be unable to fully understand, defend against and exploit the information domain.

UK Research

Work conducted as part of the UK Ministry of Defence (UK MOD), Defence Science and Technology Laboratory (Dstl) Synthetic Environment Tower of Excellence (SE Tower) provides underpinning research into the use of simulation to support training, concept development and experimentation, mission planning/preparation, test and evaluation. The SE Tower contains three Technical Columns (TCs) which are supported by Dstl and the supplier base, including industry and academia. Methods and technologies related to the Synthetic Natural and Physical Environment form part of Technical Column (TC2). This includes the Synthetic Composition and Representation of Natural and Physical Environments (SCORE) research project which is conducting research into the representation of the environment; both 'at rest' and in real time. Core team members of SCORE include XPI Simulation Ltd (Lead Contractor), Thales UK Ltd, QinetiQ Ltd and Cranfield University. The project has also engaged a wide range of other companies as 'Associates'.

Work undertaken by Thales as part of this team included a structured package of work scoping the inclusion of information warfare within simulation systems. Support was also provided to NATO Modelling and Simulation Group (NMSG) 151 – *"Workshop on Cyber Effects in Campaign and Mission Simulations"* meeting in Portsdown West in July 2017. This paper includes material from these studies and practical experiments which have not been previously published.

Under the SE Tower TC1, Architectures Interoperability and Management of Simulation (AIMS), work has been undertaken to develop the concept of providing Modelling and Simulation as a Service (MSaaS). Members of the AIMS team also including contributed to NMSG-136 *"Modelling and Simulation as a Service (MSaaS) Rapid deployment of interoperable and credible simulation environments"*. This paper draws upon material from both the AIMS and SCORE research programmes.

POTENTIAL CONCEPTUAL APPROACHES

Challenges in the Implementation of Information Warfare Simulation

Modelling and simulation practitioners face a number of challenges as they consider how information warfare simulations might be implemented. Information warfare has a number of characteristics which make it difficult to simulate. These are summarised as follows:

- **Subtle and complex -** Information warfare by definition is a nuanced and subtle business, with its effects not immediately visible. It may be more complex to model than physical warfare. Information warfare effects may be difficult to visualise within M&S support systems (such as exercise control systems or instructor stations);
- **Slow to propagate –** Some information effects relating to PSYOPS or Media Ops may be slow to propagate; with the end state not reached weeks or months after activities are instigated. This may pose challenges for exercise designers when using real time simulation, and lead to the need to run information warfare elements of an event in accelerated time;
- **Independent of space –** Some information effects can propagate through physical space quickly, particularly those relating to computer networks where effects can have a global reach. This provides a challenge when considering which physical area to select for a simulation event – a network environment may not have an obvious place in physical space;
- **Second order or 'ripple' effects –** Information effects may have secondary or 'ripple' effects on other environments. For example, offensive CNO on power infrastructure may cause damage or destruction to the infrastructure, with a second order effect on the attitudes of the local population.
- **Standards –** Existing simulation standards do not appropriately represent elements of the information environment, or the second order interactions between elements.

As a result, the need to represent information effects may result in the need to fundamentally change our approach to modelling and simulation systems. The options available are discussed below.

Potential Top Level Approaches

There are a number of top level approaches which could be adopted for the modelling and simulation of information warfare. These include:

- Abstracting complexity through approaches such as wargaming. The Camberley Kriegsspiel [6] used in the UK provides a turn based adversarial wargame which does not rely upon technology and allows information warfare elements to be abstracted. These have proven extremely effective for leadership development and to encourage intellectual agility, but probably could not be scaled up to support large exercises without significant role player support;
- Building entirely new environments which seek to model all aspects of a society, including socio-economic elements. This approach is likely to be expensive and time consuming to come to fruition and from a commercial perspective would result in 'lock in' to a single supplier. There may also be a limited ability to interface between these worlds and existing modeling and simulation systems;
- Undertaking a modular approach which seeks to append existing M&S systems with additional functionality representing the information environment. This requires effort to understand the architectures and standards required to underpin the integration of information warfare components with conventional M&S systems.

The SCORE project team has explored the third of these options, and in particular the use of MSaaS to integrate information environments into existing M&S environments.

Describing the Information Environment

As noted above, information warfare is by its nature complex and subtle. Through analysis of NATO *Allied Joint Doctrine for Information Operations* [7] and a series of thought experiments, the team sought to understand how the information domain could be described. This was intended to form the basis for an architecture around which subsequent experimentation could be conducted.

As a key underpinning principle, the information space should be understood as an environment or series of domains in its own right; where military actors can manoeuvre, contest 'ground', apply effects and have effects applied to them by adversaries. Only by treating the information environment as a dynamic and contestable environment or environments will M&S systems provide the necessarily realism, and allow commanders to apply a wider spectrum of effects. NATO doctrine [7] includes the concept of a series of six layers, which form part of three domains, creating a 'multi dimensional' environment. This is illustrated below in Figure 2.

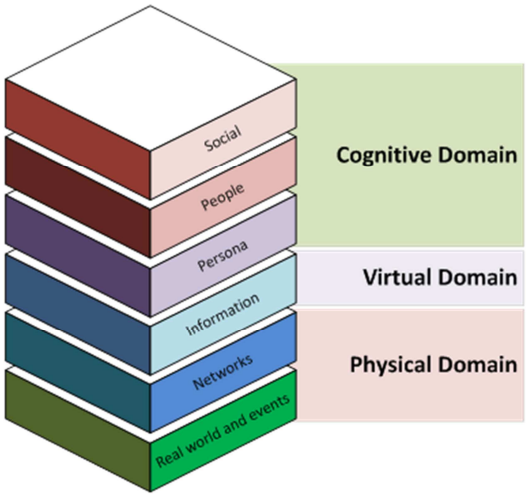

Figure 2. Adaption from [7] of NATO model containing three domains and six layers.

The physical domain is the most straightforward, and includes the physical environment such as terrain and weather, as well as a series of networks. Networks may include computer networks, communication and also physical networks associated with utilities (e.g. water, power supplies). Some of these may exist to a degree within M&S systems, particularly those associated with radio communication systems. Other Information Technology based networks are unlikely to be represented within conventional M&S systems.

The virtual domain includes information; this may include military orders or commands, and media based information. The cognitive domain contains both individuals (through people and persona) and groups (through social). Persona includes emotion based aspects such as thoughts, beliefs, desires and perceptions, along with logic based decision making. The social layer scales this up from the individual to represent groups and organisations. A representation of both key individuals (for Key Leader Engagement (KLE) for example) and groups would be required within an information warfare simulation. This cognitive domain may be represented within conventional M&S systems to a limited degree, or not at all.

Work previously carried out as part of The Technical Cooperation Program (TTCP) Joint Studies and Analysis (JSA) 2 Key Technical Area (KTA) 3 proposed a layer based model which contains four layers [8]. This is described below in Figure 3.

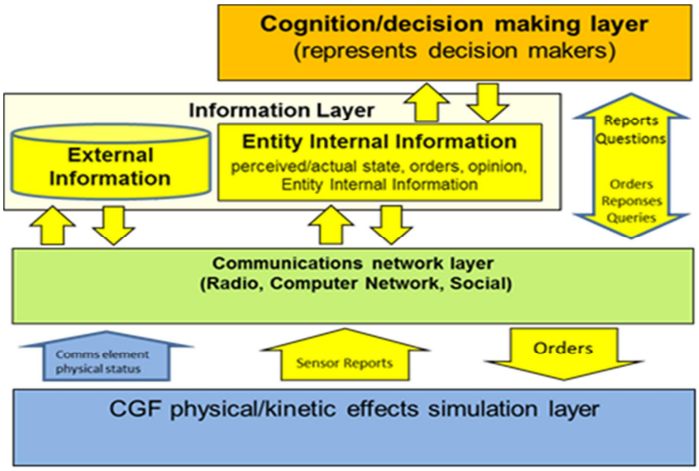

Figure 3. TTCP JSA2 KTA 3 Model from [8].

Here the bottom layer is the physical domain where physical warfare effects are provided. Above this is a network layer and information layer which also includes aspects of the cognitive domain outlined in the NATO model in the form of an entity's opinion. The top layer, the cognitive/decision making layer, includes the other elements of the NATO cognitive domain into a single cognitive layer focused on decision making.

Under SCORE, the team further developed this model to understand its component elements and the interactions between layers. An element of this was the concept of information items; individual pieces of information that could be moved between the layers, and information entities; actors who are able to produce and distribute information. A development of the TTCP JSA 2 KTA 3 model and its constituent elements is shown below in Figure 4.

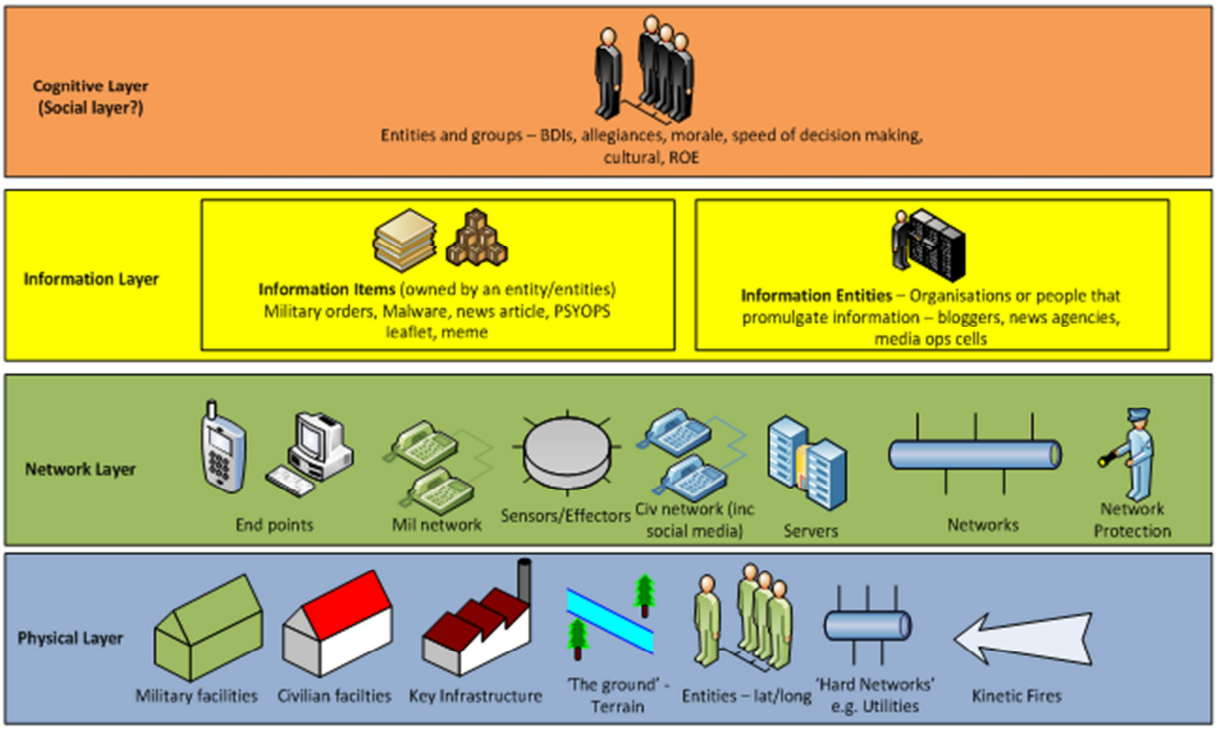

Figure 4. Development of TTCP JSA 2 KTA 3 model.

The layer model has value in that it identifies that a series of separate simulation components (in this case layers) could provide the environments and effects required of an information warfare simulation. It also provides a useful framework within which to assess existing simulations for their ability to support each layer. This concept was further developed by the team within an MSaaS paradigm.

The Modelling and Simulation as a Service Approach

MSaaS is a concept where simulation applications are provided 'as a service'. MSaaS provides the opportunity to deliver composable and easily re-configurable simulation environments assembled from common components. It also offers the opportunity to more rapidly synchronise and deploy the resulting simulations 'on demand' [9]. Work under NMSG-131 *"Modelling and Simulation as a Service (MSaaS): New concepts and service-oriented architectures"* and NMSG-136 "*Modelling and Simulation as a Service – Rapid deployment of interoperable and credible simulation environments"* supported by the team through the AIMS contract, has sought to understand the technical and organisational basis of MSaaS.

The UK MOD simulation strategy [10] envisages the use of modular run-time simulation components which can be assembled according to the user need. The re-use of simulation components across products and projects is encouraged, and common capabilities are desired in order to reduce costs and provide more opportunities for simulation interoperability. In this context, MSaaS provides an extensible and flexible framework around which common components or services can be built. In terms of information warfare simulation, MSaaS could provide a framework around which a set of common components or services representing each of the layers described in the previous section could be constructed. Specifically, this would allow other components representing the non-physical layers to be appended to a core 'conventional' simulation representing the physical domain. In this context, the each of the layers would be represented as a modular component providing a service to other elements within the simulation.

In the longer term, the MSaaS approach may facilitate information warfare simulations to be rapidly assembled and deployed in accordance with end-user requirements (be they training, experimentation, mission preparation or analysis based). For example; a CNO focused end-user could seek to select and integrate the physical and network layers as a priority, whereas a PSYOPS focused user would select and integrate a high fidelity cognitive layer.

The evolution of the layer model to a model based around modular services is show below in Figure 5. This includes a range of other services which the team identified would be needed to support the execution of information warfare simulation events, such as monitoring and control and scenario development and deployment tools.

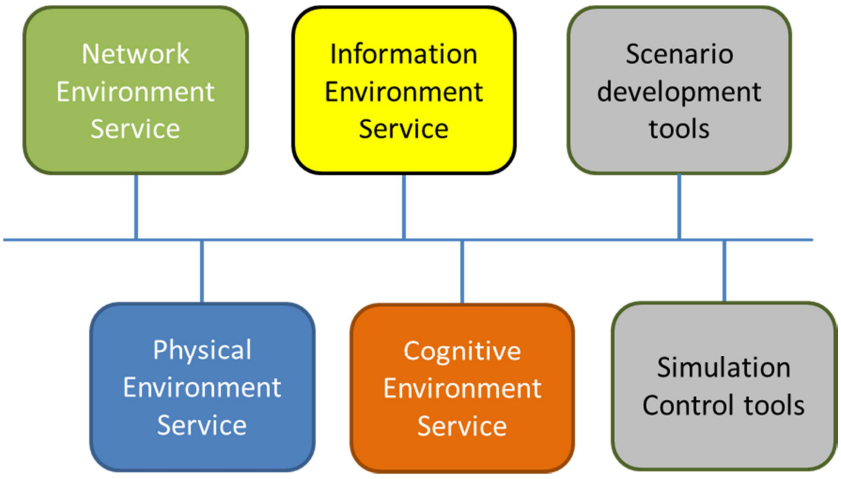

Figure 5. MSaaS based information warfare simulation model.

The SCORE project team undertook a series of thought experiments to understand and test this MSaaS based model, and specifically the interactions between the various components, before proceeding to practical experimentation as described below. Three thought experiments were conducted:

- A Media Ops scenario, where a Media Ops cell were provided by both the physical and information services. The Media Ops cell targeted an information item at the cognitive service of an audience, through the network service.
- An offensive CNO scenario, in which a CNO team target some physical infrastructure using malware. The malware (an information item) is targeted at an enemy network component, through a friendly network component. The malware is then passed from the enemy network component into the physical component.
- A defensive CNO scenario in which a CNO team look to deny access to the network service by an enemy CNO team.

Having identified through the thought experiments that MSaaS approach offered a place for each of the elements within the thought experiments, it was decided to proceed to practical experimentation, using an MSaaS approach to provide a framework for further development of the model.

EXPERIMENTATION

Experimentation Rationale

In order to better understand the implications of delivering an information warfare simulation from modular services, the team generated a test environment within which to assemble components representing the services identified above. The purpose of the experiment was not to assess each of the components for their suitability to provide the services needed, but to understand the suitability of approach as an architecture for providing an information warfare simulation. Secondary objectives were to understand the interactions between the various components in order to understand interfaces and standards, and to better scope the implications for the practical construction and deployment of these simulations. The test bed constructed is intended to provide ongoing support to other experiments within the SCORE project.

Test Bed Components

Test bed components were identified that could provide the candidate functionality required, that were easily available to the team, flexible and scalable, and which provided the functionality identified within the thought experiments described above.

- **Physical Environment.** The physical environment was potentially the most straightforward to provide, given the wide range of existing simulation tools that represent the physical domain. In line with the UK MOD simulation strategy and the principle of re-use of existing assets, the Defence Virtual Simulation (DVS) tool was utilised. This provides a virtual simulation based around the Virtual Battlespace System 3 (VBS3). VBS3 also provided an easy to modify scenario editor, and some basic behavioural functionality;
- **Network Environment.** The team sought to use a tool which could represent the technical networks within the CNO thought experiments described above, inclusive of fixed line telecoms, wireless and internet based capability. A key requirement was that this network service would need to be able to be effected (e.g. damaged and destroyed) so as to be a fully contestable environment. A network emulator was identified as the best type of tool to meet this requirement. This provided the flexibility to construct a range of network types, existing network models, the ability to degrade or damage network nodes, a Graphical User Interface (GUI) to visualise the status of networks and the potential to introduce hardware into the ecosystem at a later point. The Common Open Research Emulator (CORE), originally developed by the US Naval Research Laboratory (NRL) was selected to provide this component. Using CORE, a neutral commercial cell phone network environment was built over the physical domain with network nodes (e.g. cell towers) geolocated with points in the physical environment;
- **Information Environment.** This component required the capability to store information items and serve them to the various entities within the test bed. An in-house product, MeshDB, was used to serve information types to entities within the simulation on a client-server basis. For the purpose of the initial

experiment described within this paper, simple information types in the form of orders or commands were included within this component;

- **Cognitive Environment.** The team identified early in the study that finding a suitable tool or tools to represent the cognitive component would be challenging. Options included agent based behavioural modelling tools, Artificial Intelligence (AI) based modules or utilising behavioural or decision making based elements of other components. However, a suitable component with both the capability to model decisions and attitudes, opinions and interface with other simulation components could not be identified. As the intent for this experiment was to understand the feasibility of a MSaaS based model, the simple AI based models within DVS were used to represent the decision making element of the cognitive component appended by an 'if/then' script produced by the team, named P5. Attitudes, beliefs and opinions were not represented within this experiment; the implementation of this element is discussed further below.

The test bed included a number of other elements. These included a Common Scenario Editor (CSE), which was used to define and serve the scenario to the other components using Military Scenario Definition Language (MSDL). A simple Human Machine Interface (HMI) was also created to allow non-physical effects to be viewed. A registry and a repository were also integrated into the test bed, hosted in a commercial cloud, providing discovery and storage of simulation content respectively. The test bed utilised Distributed Interactive Simulation (DIS) protocols to pass data between components, as a number of legacy sub-systems were used which use DIS. Figure 6 below illustrates the architecture used within the experiment.

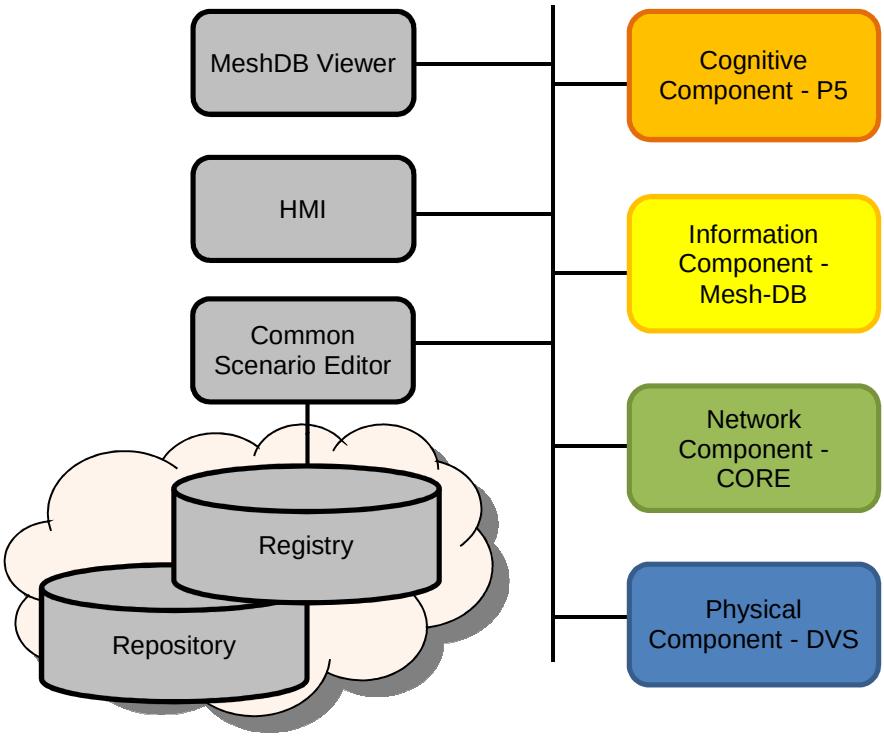

Figure 6. Test bed structure and components.

Use Cases

A series of use cases were executed using the test bed. These included:

- **Instantiation of a simple cognitive component based on perception.** A simple perception based model was created showing where a sub-unit commander believed his personnel to be, which differed from the ground truth. This delivered a simple cognitive environment providing a decision making capability;

- **Interaction between network component and physical environment.** A line of sight based model was instantiated within the physical environment based around both terrain occlusion and weather, which was linked to the network environment. This was used to demonstrate a loss of communications between a spotter who was occluded by the terrain, with the effect being observed within the network environment;
- **Interaction between physical, network and cognitive layers.** Degradation of the network component through physical damage to a cell tower in the physical component caused by a detonation event. The linkage between the network and physical components meant that damage was transferred to the network layer, reducing the effectiveness of the tower to pass messages within the network model. Damage to the network layer delayed the passage of orders from one sub-unit to another. This in turn created a second order effect within the cognitive layer, with the sub-unit in question being unreactive to orders.

Findings

The experiment demonstrated the potential viability of an MSaaS based approach with different components providing information warfare services, and demonstrated some simple use cases where effects could cascade through the different components dynamically. A number of wider lessons were learned which could offer utility to modelling and simulation practitioners. These included:

- **Scenario generation and deployment.** The use of the CSE and MSDL demonstrated that an information based scenario could be populated using existing scenario tools using existing standards. An understanding was also gained of how to programme messages to pass between the different components. However, MSDL (and in future the Command and Control Systems - Simulation Systems Interoperation (C2SIM) standard) is likely to need to be extended to encompass other elements of information warfare scenarios not currently covered by the standard;
- **Content population.** The introduction of three non-physical components existing alongside the physical environment significantly increases the amount of content that needs to be generated. Conventional simulations tend to be populated with geospatial information (e.g. the topography of physical terrain) and Order of Battle (ORBAT) information. Information warfare simulations are likely to need to draw upon wider non-traditional sources of content, which may be as varied as open source or classified infrastructure information and social or open source media information. This has the potential to increase the time taken to generate and populate scenarios, and may have legal or policy implications if personal data is used to populate environments. Furthermore, M&S practitioners may not be able to utilise classified information relating to Critical National Infrastructure to populate hard networks such as power or utilities. Within the experiment, the team utilised fictitious infrastructure for this reason;
- **Supporting tools.** During integration, the team realised that an HMI was required in order to visualise information effects and entity states, as this functionality was not supported by the existing components. Especially where information warfare simulations draw upon non-modelling and simulation native tools (such as AI models for the cognitive component), new components will need to be delivered which visualise information effects. For the cognitive component, these could draw upon intelligence based products, such as the Shade shift, showing affiliation of audiences and actors within the battlespace. The visualisation of these effects will be a key factor in communicating the value of information warfare simulations to end users;
- **Network environment.** The experiment demonstrated that a network emulator could provide a representative network component and that network nodes (e.g. cell towers) could be correlated with entities in the physical environment. This allowed the destruction and degradation of elements of the network and a demonstration of 'ripple effects' within a dynamic environment. Due to time constraints only a 'neutral' network environment could be created. Further work could generate 'friendly' and 'enemy' network environments to allow attack and defence scenarios to be generated, and expand into other network types. The HMI provided by these tools is also a useful capability in visualising the network environment and any effects;
- **Information environment.** MeshDB provided a centralised information store within the experimentation infrastructure. This provided a scalable information service to the other components, and it was successfully demonstrated that information items could percolate through the other components. This demonstrated that a library based information environment could constitute the information component;

- **Cognitive environment.** The experiment provided a very basic rules-based cognitive environment. This remains the most immature of the components demonstrated, and provides a technically challenging component to represent. Further work is required to scope this element and its interaction within more complex use cases.

CONCLUSIONS

As information warfare becomes an increasingly central part of military operations, Simulation systems and SEs will need to evolve to better represent it. However, the information environment and information effects are by their nature ambiguous and difficult to simulate, especially as they relate to human behaviours and thought processes. In order for commanders to exercise a wider spectrum of information effects integrated with physical effects, dynamic environments are required within which forces can manoeuvre and implement effects.

MSaaS provides a possible approach for representing these dynamic environments to provide simulation of information warfare, assembled from different components. It offers the potential to generate scalable information warfare simulations that can be quickly brought together and tailored to end user needs. Tools to provide some of these components, such as those for the network environment, are relatively plentiful. For the cognitive environment, mature solutions appear to be in short supply; but could leverage AI technology. This remains the most challenging area to address.

Supporting tools such as those required for exercise control, scenario generation and After Action Review (AAR) will also need to be developed to support the deployment and delivery of information warfare simulations. In particular, these may need to be extended to allow 'soft and subtle' type effects to be visualized by participants and M&S practitioners. Current standards for scenario generation and simulation interoperability may need to be extended to incorporate information warfare effects; particularly messaging targeted at populations as part of psychological operations and media operations. Content generation for these environments may have to explore wider sources of information such as the use of open source media; these sources may have restrictions on their use for reasons of security or personal data.

In summary, the use of MSaaS to provide information warfare simulation becomes a challenge of integration between dissimilar components, and a challenge of populating unfamiliar environments with the right type of data. Information warfare is not going away; and the extension of our current M&S environments will need to proceed at pace to represent it.

ACKNOWLEDGEMENTS

The team would like to acknowledge and give thanks for the support of our Dstl sponsors, Neil Smith, Bharat Patel and John Lloyd. The team would also like to thank Mark Hazen and his team from Defense Research and Development Canada (DRDC) for his advice and thought leadership in this area and to wish him a happy retirement.

REFERENCES

[1] The Art of War by Sun Tzu. Retrieved 12 April, 2018 from: http://classics.mit.edu/Tzu/artwar.html
[2] Hybrid warfare – does it even exist. Retrieved 12 April 2018 from https://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/
[3] Countering Information war – Lessons learned from NATO and partner countries. Retrieved 12 April 2018 from https://www.globsec.org/wp-content/uploads/2017/09/countering_information_war.pdf
[4] Berkowitz, B. Warfare in the Information Age, Issues in Science and Technology Vol. 12, No. 1 (FALL 1995), pp. 59-66
[5] Joint Doctrine Publication 3-00, Campaign Execution, Third Edition
[6] The Camberley Kriegspiel: A Wargaming Tool. Retrieved 13 April 2018. https://chacr.org.uk/docs/The-Camberley-Kriegsspiel-Article.pdf
[7] Allied Joint Publication (AJP) 3.10 – Allied Joint Doctrine for Information Operations. November 2009.

[8] Hazen, M. Lloyd, J. & Page, E. The Evolution of Computer Generated Forces (CGF) Architectures to Support Information Warfare Effects. STO-MSG-143, undated.
[9] STO Technical Report: Modelling and Simulation as a Service (MSaaS) – Rapid deployment of interoperable and credible simulation environments. Final report of NATO MSG-136. STO-TR-MSG-136, undated.
[10] Defence Concepts and Doctrine Centre (DCDC). Defence Policy for Simulation. CDP/4/3/DCDS (MilCap)/15/Apr/34. April 2015.