The Representation of Information Warfare effects in the Synthetic Battlespace

Keith Ford **Deryck Arnold**
Thales UK
Crawley
UNITED KINGDOM

keith.ford@uk.thalesgroup.com deryck.arnold@uk.thalesgroup.com

ABSTRACT

The current generation of Simulations and Synthetic Environments (SEs) focus on physical warfare effects and do not adequately represent the wider spectrum of activities in the operational environment. In order to provide a more realistic environment, the next generation synthetic battlespace must include a better representation of other aspects of operations including information warfare, infrastructure, logistics, human interactions and the general populace.

Thales has led a project on behalf of the Defence Science and Technology Laboratory (Dstl) in the UK to research the provision of Information Warfare effects in the synthetic battlespace. This includes the ability to deny, degrade, corrupt or destroy the enemy's sources of information whilst preserving its own. The future synthetic battlespace must also enable synthetic entities to change their behaviour as a result of the information they receive through sources such as web sites, social media, television and radio.

To promote the reuse of Modelling and Simulation (M&S) across the defence community, the UK MOD has a desire to move away from monolithic simulations to more component architectures when representing the synthetic battlespace. In keeping with this approach, Thales has developed a 5 layer communications model in which the information can be manipulated at different stages of the communications chain.

1.0 INTRODUCTION

The aim of the UK Defence Science and Technology Laboratory's (Dstl) Simulation Composition and Representation of Natural and Physical Environments (SCORE) project was;

'To inform the development of coherent and consistent synthetic representations of the operating environment to provide more effective defence capabilities in support of training, concept development and experimentation, through-life acquisition and evaluation.'

The programme comprised a number of work packages that investigated the representation of weather effects and behaviours in simulation environments, and the reuse of simulation components. This paper describes the research Thales UK performed on investigating how information warfare effects can be introduced into simulation systems.

In the context of this paper, the word simulation is used to refer to a complex distributed simulation that is used to stimulate operational equipment.

1.1 Background

The current generation of distributed simulations focus on physical warfare effects and do not adequately represent the full gamut of activities in the operational space. In order to provide a more realistic environment, future simulations must include a better representation of other aspects of operations including human behaviour (e.g. sentiment, relationships, interactions), information warfare (e.g. cyber and psychological operations using social media, television/radio), infrastructure (e.g. electricity, gas, water, communication, food distribution, road and rail network), populace (e.g. number of people/vehicles, individual and group behaviours).

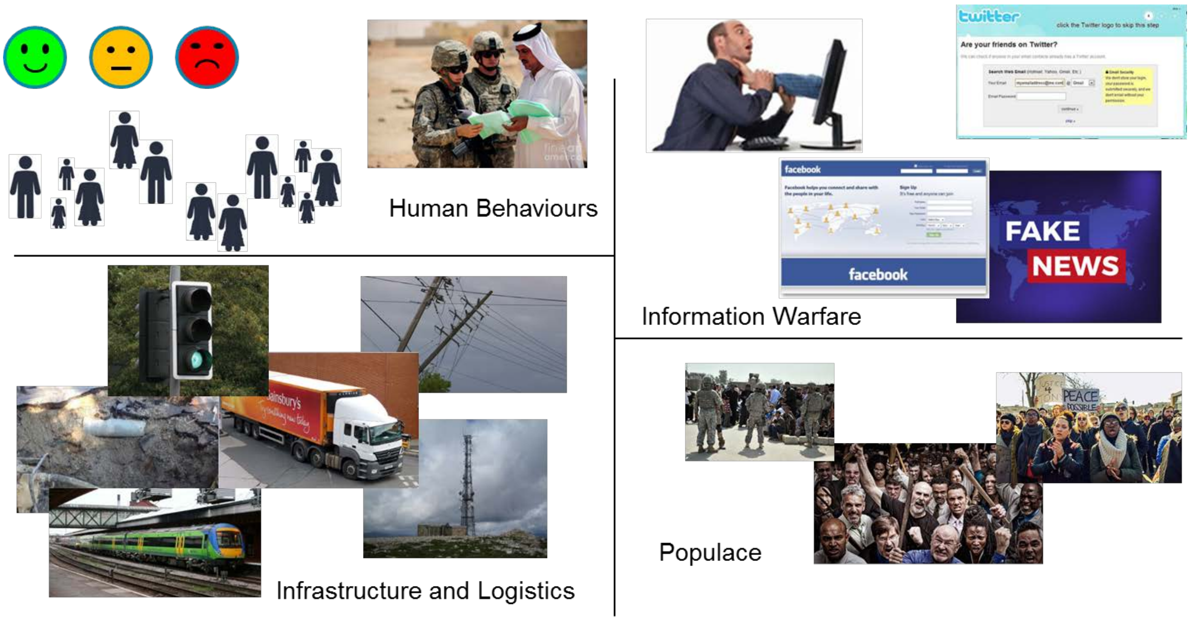

Figure 1 Capabilities Required in the Future Synthetic Battlespace

1.2 Information Warfare

In lieu of an agreed definition of Information warfare (IW), for the purposes of this paper, it is defined as ‘a concept involving the battlespace use and management of Information and Communication Technology (ICT) in pursuit of a competitive advantage over an opponent’ [1]. There are six aspects to Information Warfare;

- Physical information warfare – Denial of information to an adversary by physically destroying components of the information system;
- Electronic warfare - Denial of information to an adversary using electronic methods e.g. jamming;
- Psychological operations - Affect the state of mind of adversaries by using information against them;
- Military deception – Using information to make the adversary believe own capabilities and intent is far greater than they really are;
- Information attacks - Corrupt information without changing its original structure and location so that the recipient is unaware that it has been altered;
- Security measures - Prevention methods used in order to protect the information system so that it is not breached by an adversary.

Communication of information can be delivered by various means including visual, oral, and written and can be transmitted point-to-point or broadcast. However delivered, in the modern operational space, the propagation of information can be blocked, delayed or changed. This capability is used both by friendly forces and adversaries to influence the outcome of a campaign. It should be noted that the term information also includes the transmission of data i.e. information without context.

Future training systems must be able to represent all the different aspects of Information Warfare. However, there is a clear challenge in extending traditional approaches to simulation to satisfy these new requirements. Reference [2] describes the development of a conceptual model to support information and cyber warfare effects in modelling and simulation systems. The inclusion of Information Warfare effects needs to be seamlessly integrated with kinetic effects in future simulation environments.

A new 'weapon' available to both the military and adversaries is the use of Fake news, which is typically spread through broadcast systems such as TV, radio and web sites. The purpose of fake news is to surreptitiously alter the views of individuals, groups and the general populace. This can be used by the military to try and win-over the populace. Likewise it can be used by adversaries to turn the populace against say a peacekeeping force. As an example, misinformation about food handouts not complying with local religious practices could be generated to alienate a Peace Keeping Force from the local populace. Therefore, a commander needs to disrupt the flow of information and/or counteract it with messages that will neutralise the false messages.

1.3 Previous Research

Work within The 'Technical Cooperation Program (TTCP) Joint Studies and Analysis (JSA) 2 Key Technical Area (KTA) 3' proposed a layer based model for representing information warfare effects as shown in Figure 2 [3].

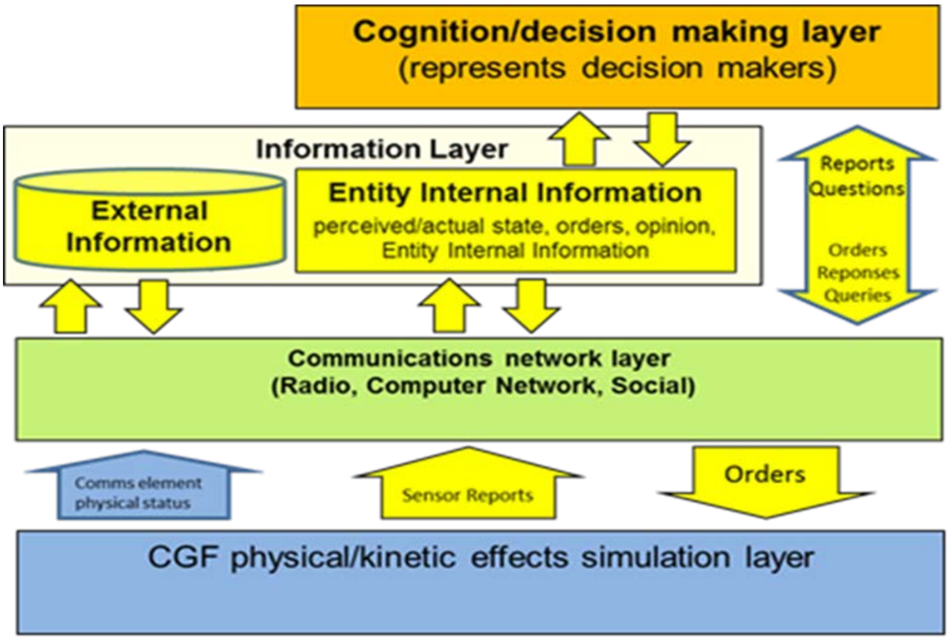
Cognition/decision making layer
(represents decision makers)
Information Layer
External Information
Entity Internal Information
perceived/actual state, orders, opinion, Entity Internal Information
Reports
Questions
Orders
Reponses
Queries
Communications network layer
(Radio, Computer Network, Social)
Comms element physical status
Sensor Reports
Orders
CGF physical/kinetic effects simulation layer

Figure 2 TTCP JSA2 KTA 3 Model

In the above model, there is a transition from physics-based to cognition-based processes (bottom to top). So the physics-based aspects of electronic attack and Cyber can be implemented in the Communications/

Networking layer, as would the removal of a key commander in a hierarchical command structure. The interception or modification of information content type of attacks would take place in the Information Layer, and finally, decision making processes are implemented in the top layer. Thus, EW and Cyber primary effects are applied at the middle two layers, but secondary and tertiary effects are driven by the modelling of the upper two layers and would manifest (be visualised) in the bottom layer as entity behaviour.

2.0 INFORMATION WARFARE IN THE SYNTHETIC BATTLESPACE

Whilst aspects of Information Warfare have been represented in simulators for a long time e.g. jamming communications, the current representation of communication systems is not sufficient to satisfy the latest needs. As an example, the use of more sophisticated representations of information systems is particularly required in large collective exercises where a commander and their team are being trained in a representative HQ (Figure 3).

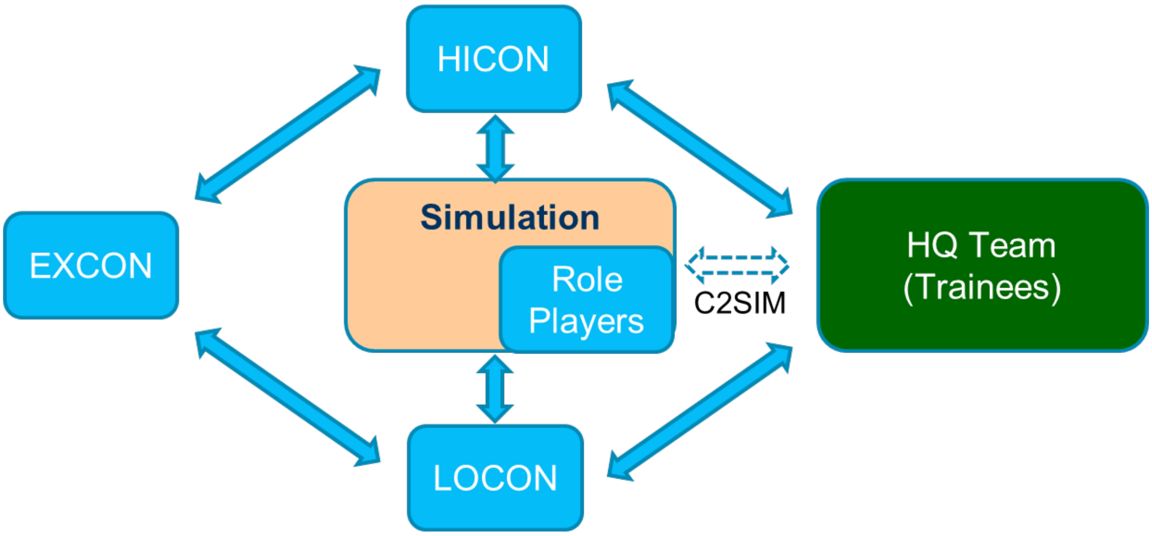

Figure 3 Elements of a Representative Exercise

In Figure 3, the simulation could be a large monolithic application or a complex distributed set of simulators and simulations. The ideal situation is where the HQ team use their normal operational C2 systems that are stimulated directly by the simulation using protocols such as C2SIM [4]. Currently the translation between the operational equipment and the simulation is mostly performed manually by the LOCON and HICON.

The EXCON is responsible for ensuring the training objectives are satisfied and for ensuring events from the Master Events List (MEL) are injected at the appropriate time. Depending on how well the HQ team are performing, the EXCON may also scale back or increase the complexity of the situation the commander has to deal with. The injects are passed to the LOCON who make the appropriate changes to the simulation e.g. evacuation helicopter crashes. The LOCON will also pass information from the simulation to the C2 systems in the HQ. The role of the HICON is to make decisions regarding the upper echelons in the chain of command. The HQ commander will report to them and they will feed back orders based on the political and strategic landscape. It should be noted that as well as a commander trying to disrupt information flow amongst adversaries, the effect of adversaries disrupting the information flows coming from and being sent to the HQ can also be disrupted.

From an information warfare perspective, the lines of communications that need to be represented in a simulation include those between:

- HQ commander and upper/lower echelons in the chain of command;
- Platforms e.g. Link16;
- Individuals e.g. military personnel, insurgents and civilians;
- Groups of people e.g. military personnel, insurgents and civilians;
- General populace.

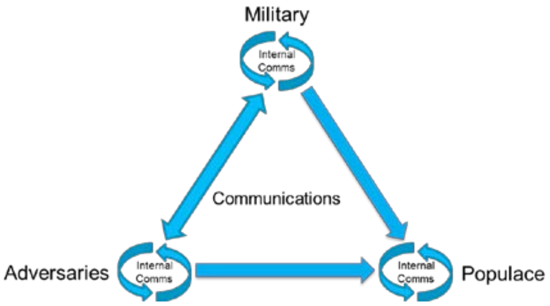

Figure 4 Lines of Communication

Information is transmitted using different media and the simulation environment should be able to disrupt the flow of information no matter how it is transmitted including:

- E-mails
- Texts
- Mobile phone / Telephone
- Personal radio
- Web sites
- Social Media e.g. Facebook, Twitter, LinkedIn
- TV / Radio

Commanders need training to understand what tools and techniques they have available to disrupt information flow between adversaries or even the population. In addition, they need to understand the importance of protecting studios for broadcast systems such as TV and radio to ensure that they are not overrun by adversaries who could send out their own messages. Where adversaries have the capability for sending out broadcast messages the commander needs to use their ability to jam the signals. Web sites providing official information need to be properly protected against cyber-attacks. Conversely, web sites promoting anti-government information need taking down.

3.0 5 LAYER COMMUNICATIONS MODEL

Figure 5 shows a logical mapping of different aspects of the battlespace onto 3 orthogonal domains.

Environment Domain – Represents the physical location and state e.g. operating/destroyed, of entities (platform and people) and infrastructure e.g. communication network, in the real and synthetic environment.

Cognitive Domain – Decision making by EXCON, exercise participants, role players either by real people or using Artificial Intelligence (AI);

Information Domain – Information flow through communication system;

A key facet of the model is that the inclusion of an information warfare capability doesn't disrupt the way existing '2 dimensional' simulations currently operate.

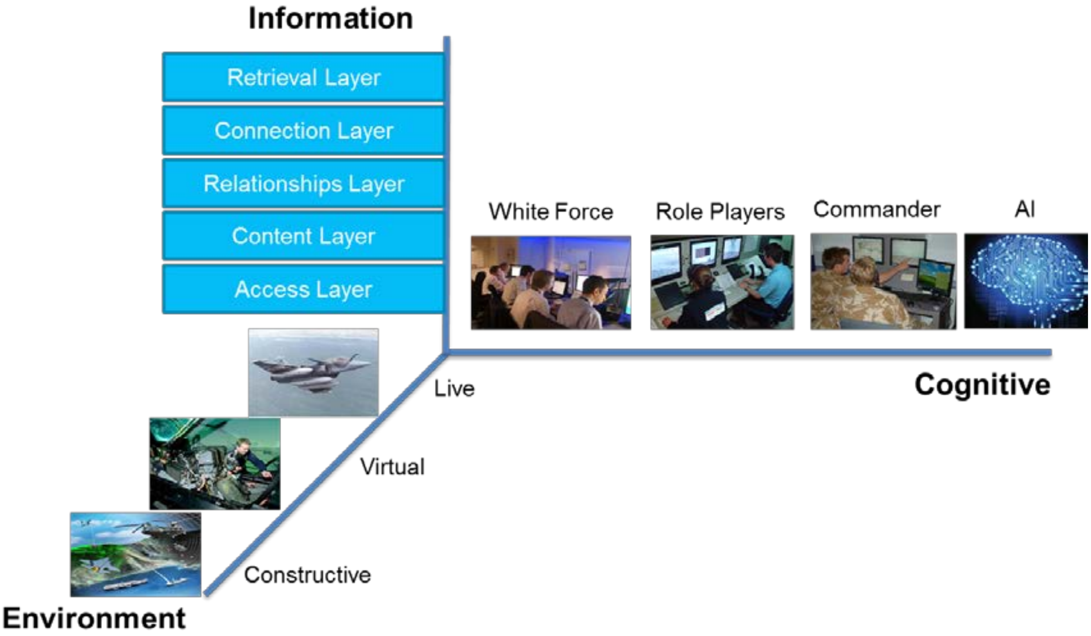

Figure 5 3 Axis Battlespace Model

The Environment domain includes operational C2 equipment and any physical infrastructure used by an exercise. The synthetic environment provides a wrapper to extend the physical environment of the HQ and represents all entities and infrastructure in the battlespace. Sensors in the synthetic environment typically stimulate the operational equipment used by the war fighters in the HQ. With respect to information warfare, the environment layer is responsible for representing the physical elements of the communication systems. These include the laydown of the communication bearers in the terrain e.g. copper or optical fibre cabling, intermediate network elements such as communication towers and the physical location of operator terminals. The Environment domain provides the means for disrupting communications using kinetic effects e.g. ordnance falling or being planted close to communication equipment that will render it inoperable. It also determines if a person represented by a CGF has an appropriate device for sending a communication e.g. are they carrying a mobile phone.

The Cognitive domain is where information from the Environment and Information domains is received and where decisions are made. These are made by commanders in the HQ who are endeavouring to accomplish the goals of the exercise. The EXCON may decide to introduce effects to challenge the commander and role players will make decisions to achieve the objectives they have been given. To reduce the number of white force players (i.e. all those supporting an exercise), which can be very costly, the use of more advanced AI techniques is being exploited in simulation environments.

The Information domain takes into account and isolates the factors that can disrupt the flow of information in the operational space. It is applicable to messages sent by any real or constructive people participating in or supporting an exercise and all the different forms of communication media.

The 5 Layer Logical Communication model is part of the Information Domain. The model was originally developed by SCORE [5] and has been further adapted as a result of writing this paper. It effectively provides a generic approach to representing the functionality of the 'Information Layer' described in [3].

The following provides a brief description of the information layers, which are described in more detail in the following sections.

Access Layer – Determines if people have access to a communication device;

Content Layer – Provides the ability for the message's recipient or sender to be changed, or for the content of the message to be altered;

Relationships Layer – Identifies groups/communities of users that are able to communicate with each other e.g. Skype address book;

Connection Layer – Determines if there is a path through the communication network between the sender and recipient of a communication;

Retrieval Layer – Represents the delays associated with when a message is accessed and acted upon.

A prerequisite for a person to be able to send or receive a message is that they must have access to either physical or simulated communication equipment, which would be represented in the Environment Layer. Information flows from the sender's communication equipment through to the Connection Layer and then to the receiver's communications device also represented in the Environment Layer.

In order for a person to successfully receive a message over a communication network, the following conditions must be satisfied:

- Access Layer - Sender/receiver must be physically close to or holding the communications device being used;
- Content Layer: Message 'header' or content must not have changed;
- Relationships Layer: The receiver must be in the same user group as the sender;
- Connection Layer: At least one communication path must exist between the sender/receiver;
- Retrieval Layer: Receiver must look at communications device.

It should be noted that as a logical model there may not be a one-to-one mapping between each layer and a service that provides the desired functionality. In some instances a single tool may be sufficient to represent the effects of all the layers.

3.1 Access Layer

The Access Layer determines that when a person wants to communicate with somebody else, both sender and receiver have access to a suitable communication device. This can be achieved automatically by interrogating the Environment to determine the location of the communication equipment and people using it. The output from the Access Layer service is True /False corresponding to whether the communication can occur or not.

3.2 Content Layer

The purpose of the Content Layer is twofold; to provide the ability for the name of the recipient or sender to be changed and to change the content of a message without the sender or receiver necessarily knowing what has happened. This enables the effects of spoofing to be simulated, which is the forgery of an email header so that the message appears to have originated from a legitimate sender rather than the actual fraudulent source. Information about people such as mobile numbers for texting, e-mail addresses, social media usernames and passwords is commonly obtained using social engineering tactics. E-mail spoofing is a popular tactic used in phishing and spam campaigns because people are more likely to open a communication when they think it has been sent by a legitimate or familiar source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation [6]. A spoofed email may also include a link that installs malware on the recipient's device if clicked.

The Content Layer also enables the content of the message or web site to be corrupted by simulating attacks on the communication system. Making parts of the message unreadable could lead to misinterpretation of the message resulting in commanders making incorrect decisions. If the communication system is compromised by an adversary, the tactic of subtly changing the content of the message may be used to tarnish the image of the impersonated sender e.g. peace keeping force. This capability could be used to alter the mood of enhanced behaviour models.

A simple Content Layer service would store a message in a queue to be manually processed and forwarded by the HICON or LOCON. This will enable them to change the message header or content so they are commensurate with the objectives of the exercise. The use of AI techniques to understand the message content may in future provide some form of automatic or at least semi-automatic way of changing the content of the message. The fidelity of the spoofing attacks to be simulated will be dependent on the objective and scale of the exercise being performed. However, it is conjectured that in most situations it will not be necessary to actually represent the content of the message but only its effect.

3.3 Relationship Layer

The Relationship Layer defines which people are able to communicate with each other. For text messages and e-mails it would define who is in their list of contacts. For social media it would specify what groups they are associated with. This function influences how messages are spread throughout the populace when sent to many people in an address book.

The input to a Relationship Layer service could simply access a spreadsheet that contains the names of the key players in the exercise, who is in their contact list and what groups they belong to. A more sophisticated implementation could implement it as a relational database. When a message is received, the Relationship service would check the message header to see if the sender and receiver are known to each other. If not, the message is discarded and not passed onto the Connection Layer.

3.4 Connection Layer

The Connection Layer controls the ability to transmit a message as a result of the interconnections and operational state of components in a communication network. This includes the communication bearers e.g. copper cables, optical fibre, and network components such as access points, switches and servers. Key components in the Connection Layer should have a corresponding representation in the Environment domain. This is to enable these components to be destroyed or disabled by activities that take place as the scenario unfolds.

Connectivity can be affected by several effects including:

- Loss of power;
- Elements of the network infrastructure being destroyed;
- Electronic warfare e.g. jamming;
- Loss of line of sight e.g. between VHF transmitters/receivers;

- Weather e.g. affecting atmospheric propagation of the electro-magnetic spectrum;
- Cyber-attacks e.g. denial of service.

The Connection Layer is initialised by storing the physical location of all the network elements being modelled and key personnel (constructive or role player) participating in the exercise. During an exercise, it receives the status of the communication equipment i.e. operating/destroyed from the Environment domain. It also receives the updates to the location of mobile communication devices and that of key personnel. This is important as it is used to determine whether a person has the means and is able to communicate with somebody else in the exercise. This could be due to being out of range or not having line of sight to a communications tower, or they are not next to or are carrying a communications device. For people speaking to each other without the aid of any communication equipment, the connection layer determines if they are physically close so could reasonably be expected to talk to each other.

COTS and open source network emulators are currently available that provide the required functionality for representing communication networks. These can be interrogated by a Connection Layer service to determine if there is connectivity between two communication devices. In order to degrade the transmission of a communication signal due to low bandwidth or jitter, the output from operational equipment can be passed through a network emulator.

Communication systems can be very complex with redundant paths and elements to provide resilience. However, it should always be borne in mind that the simulation should not be more complex than is needed to represent the desired effect. For some exercises, a realistic simulation of the key components in a network may be required to represent the effect of a denial of service attack overloading a server. In other exercises it may only be necessary for the EXCON to inject an event stating that a cyber-attack has taken place and that no messages will be transmitted through the Connection Layer.

3.5 Retrieval Layer

The Retrieval Layer simulates the real world latencies related to when people receive and process messages. With respect to receiving text messages on mobile phones, this could be because someone has their phone on ‘Do Not Disturb’ or they just miss the notification. When messages are propagated by social media e.g. Facebook, it can represent the delay in reading and forwarding messages. For information spread via web sites, the latencies relate to how often people would look at a particular page. For broadcast messages, it corresponds to whether someone or a group of people is watching or listening to the TV or radio (in this case, the message would either be received or not received).

The requirement of a Retrieval Layer service would be able to control the delay before the message can be accessed by the communication device. The delay could be produced using a random number generator that is initialised to control a delay profile for each participant and/or message.

4.0 SCORE EXPERIMENTATION

SCORE experimented with how existing and new services could be combined to represent Information Warfare effects in a simulation.

4.1 Degradation of Communications Using Real Equipment

To demonstrate how the performance of real operational equipment can be degraded in an exercise the communication path for a Skype call was routed through a network emulator. The network emulator provides the ability to degrade the signal by altering the amount of jitter and latency experienced by the transmitted data. This manifested itself as a poor quality video and voice, which made it harder to communicate. The communication link was finally lost when the latency was too great.

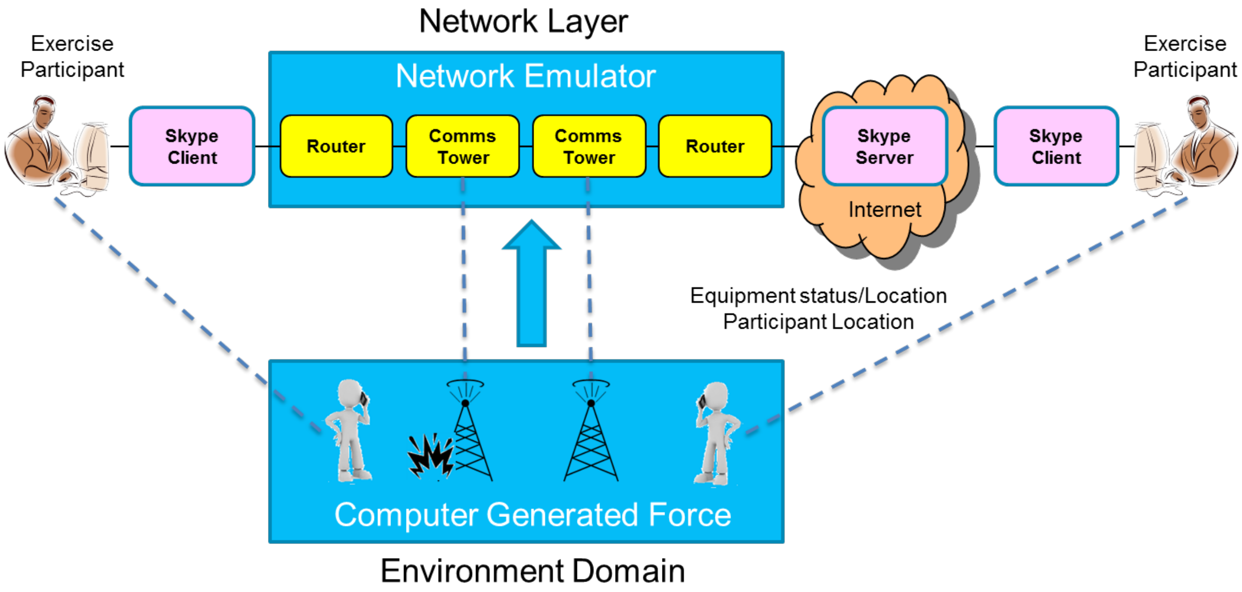

Figure 6 Degradation of Communications Using Real Equipment

The network emulator had an Application Programming Interface (API) that enabled the attributes of communication elements being modelled to be controlled programmatically. This ability was used to control the status of a communications tower and to change the location of the sender and receiver. As the sender and receiver moved out of range of the communications tower, as determined by the CGF, the Skype signal was lost. It was also lost when a kinetic effect represented by the CGF in the Environment domain caused one of the communications towers to be destroyed. In addition to video and voice calls, the approach is also applicable to sending e-mails and texts.

4.2 Message Propagation

The Message Propagation experimentation explored the use of a Connectivity service to determine connectivity between two entities by interrogating a network emulator (Figure 7). This was used to demonstrate the effect of a text message being propagated around a group of people. In this case the message is not actually sent through the network emulator but the ability to send message is indirectly affected as a result of there being a path between the sender and receiver or not.

During initialisation, the actual position of 3G/4G base stations in the area of interest, which was derived from government data, was downloaded to the network emulator. Entities were created in the network emulator to represent people in the scenario that had mobile phones and their location was updated in real-time by the CGF.

SCORE developed a Propagation service that could be configured to represent latencies related to when people would have read and forwarded a message. The Propagation Service provided the identity and location of the sender and receiver as inputs to the Connectivity Service. This interrogated the network emulator to determine if people represented in the CGF were within range of a 3G/4G base station to be able to receive or send messages.

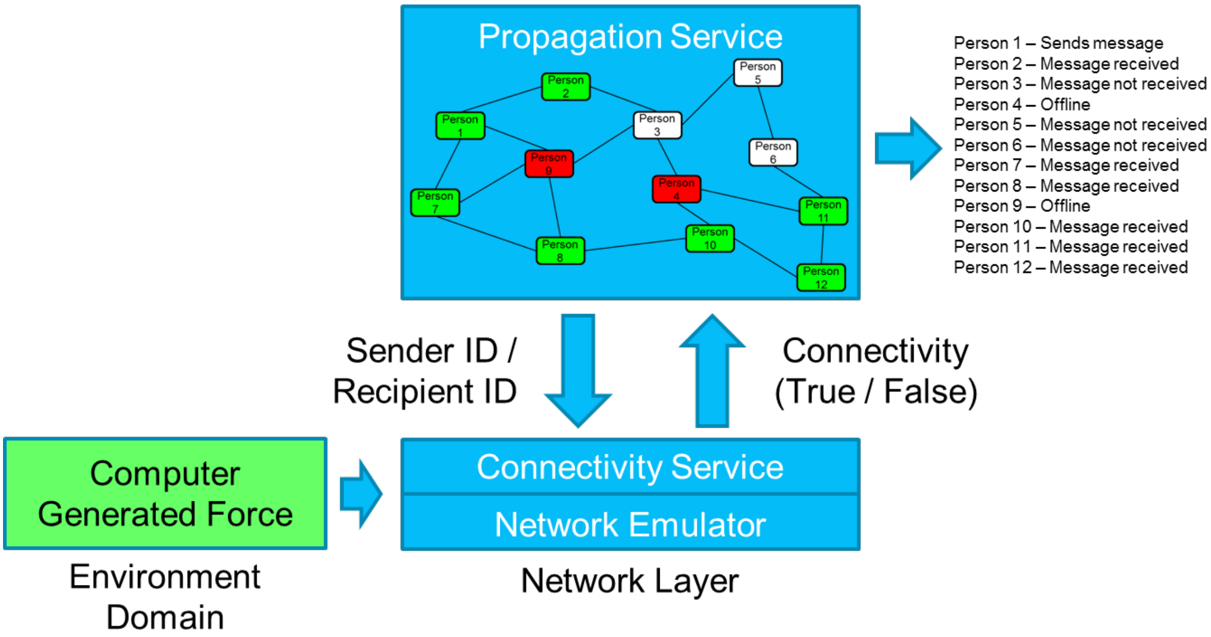

Figure 7 Demonstration of Message Propagation

The Propagation Service was initialised with random delays to represent when a person looked at a message and when they forwarded it. To demonstrate propagation delays, the Propagation Service displayed icons, representing the people in the scenario, which changed colour when messages were received. As people moved around they would come in and out of the range of the base stations and their icon turned red until connectivity was re-established and green when they received a message.

The Connectivity service was integrated with the CGF using the High-Level Architecture Evolved (HLA-E). By isolating the network emulator from the rest of the simulation, it has the advantage that if a different network emulator was used, it is only necessary to add another interface to the Connectivity service and it is not necessary to change the interfaces of other services that require access to it.

5.0 CONCLUSIONS

The current generation of Simulations and Synthetic Environments (SEs) focus on physical warfare effects and do not adequately represent the wider spectrum of activities in the operational environment. In order to provide a more realistic environment, the next generation synthetic battlespace must include a better representation of other aspects of operations including information warfare, infrastructure, logistics, human behaviours/interactions and the number of people represented in a simulation. The future synthetic battlespace must also enable synthetic entities to change their behaviour as a result of the information they receive through sources such as web sites, social media, television and radio.

The inclusion of information warfare effects greatly increases the realism for simulating the modern operational space as it can better represent the 'fog-of-war'. In future simulations, when a commander sends an order, it cannot be assumed that the recipient will receive it immediately or at all. It might even be that the message itself has been interfered with. The inclusion of more representative communication models will increase the scope of training that can be performed. The SCORE experimentation showed that it is possible to provide an information warfare capability by integrating new capability to the existing approach to simulation, which enables it to be retrofitted to legacy simulations.

The 5 Layer Communication Model described in this paper extends the TTCP JSA2 KTA 3 model by providing a structured approach to degrading and corrupting communications. It is relevant to all types of communication media e.g. e-mails, texts, social media. Isolating the factors that affect the ability to transmit messages into these layers facilitates a more representative method of disrupting communications than can currently be represented in simulations. It also has the advantage that each factor can be changed independently and that the effect is automatically propagated to any other services that use communications. As an example, if a communications component e.g. communications tower, is immobilised by physical or cyber effects, it will not be possible for any communication devices using that network element to be able to pass messages (unless there are redundant paths).

The communications model is a logical model and that there does not have to be a one-to-one mapping between the different layers of the communications model and the services/applications providing the required functionality. For example, as some CGFs are now able to represent networks as well as entities such as people and platforms, the functionality provided by the CGF may span several layers. The provision of the functionality required by each layer of the communications model could be provided as a service, which is commensurate with NATO desire to provide Modelling & Simulation as a Service [8]. The services should have a user interface so that their effect can be manipulated during an exercise by the white force but more importantly, they should have an Application Programming Interface (API), to enable changes to be made programmatically.

The inclusion of information warfare in a simulation means that in future, scenarios will need to support additional data types e.g. for defining network topology. Further research is needed to identify the functionality required by services supporting the 5 Layer Communications Model, and to agree standards for exchanging information. Where possible, existing standards should be employed such as the use of Shape files for defining the physical routing of the network infrastructure and Digital Terrain Elevation Data (DTED) for defining the terrain. In future, network emulators need to be able to receive and respond to weather effects using the standards being defined by MSG-156.

There is an old adage that says 'every model is wrong, but some are useful [7]. The art of simulation is just providing sufficient fidelity to satisfy the requirements without producing a 'gold-plated' solution. Whilst the need to be able to better represent information warfare effects in simulation environments has been recognised, the solutions employed can be very different. The criteria for what kind of solution is to be employed, is very dependent on the effect it must achieve. In some cases, it may be sufficient just to block a message getting through or it may only be necessary to simulate the effect of sending a message rather than its content e.g. it changes someone's allegiance. If the timing of a message is important to an exercise then a more sophisticated simulation is required to represent latencies in the transmission and receipt of messages. Future systems for providing Information Warfare training should be able to represent all the tools available to a Commander and the effect of their actions or inaction; did it prevent or cause an attack taking place, has it reduced or increased tensions in the population did they target the correct person or group of people?

The SCORE experimentation demonstrated different solutions for implementing the 5 Layer Communication Model; communications could be degraded by passing information through a network emulator or its output used indirectly to affect communications. The approach to be used in an exercise is dependent on the type of communication being transmitted and the requirements for the simulation. SCORE demonstrated that by passing information through a network emulator, it is possible to degrade e-mail and text video/voice streams sent via operational equipment that is used in an exercise. This enables communications in the chain of command to be disrupted i.e. between a Commander and the HICON/LOCON, and between other participants in the exercise.

The inclusion of information warfare effects in a simulation will require more advanced behaviour models for constructive entities so that they can respond to the effect of the communications. These would be associated with the Cognitive domain. SCORE demonstrated the use of a 'Disposition' service that altered the mood and allegiance of constructive entities depending on the information they received [5]. In the future, constructive entities rather than the LOCON should be able to automatically generate messages that create the background traffic that are used to mask important messages that a Commander should react to.

The SCORE experimentation has shown that the High-Level Architecture (HLA) and Distributed Interactive Simulation (DIS) are appropriate for communicating the location of entities from a CGF to a network emulator. The use of network emulators will provide a quick-win for representing the disruption of communications in simulations. It is recommended that new standards should first focus on producing a standard for initialising and controlling network emulators as there is a danger of a plethora of proprietary standards emerging for these tools. SCORE demonstrated the use of a network service that could be used to provide a common interface to different network emulators, which could provide an intermediate solution until standards become available.

As well as the network emulators representing communications networks, they could also be used in future to simulate utilities such as power distribution and water networks. Infrastructure such as electricity sub-stations and pumping stations could also be represented in the Environment Layer. The effect of these utilities not being available could be used to negatively affect the mood of the populace, which could change the outcome of an exercise.

ACKNOWLEDGEMENTS

The authors would like to thank Dstl and the SCORE team for directly or indirectly influencing the ideas presented in this paper.

BIBLIOGRAPHY

[1] “Information Warfare,” [Online]. Available: https://en.wikipedia.org/wiki/Information_warfare.

[2] J. Kearse, “Development of a conceptual model to support information and cyber warfare effects in modelling and simulation systems,” in NATO NMSG-151, Dstl Portsdown West, 2017.

[3] Various, “TTCP Technical Report: Implementation of Information Layer Warfare Effects in Computer Generated Forces (CGF) Simulations, TR-JSA-2-2016,” The Technical Cooperation Programme, 2016.

[4] “C2SIM PDG/PSG - Command and Control Systems - Simulation Systems Interoperation,” Simulation Interoperability Standards Organization, [Online]. Available: https://www.sisostds.org/StandardsActivities/DevelopmentGroups/C2SIMPDGPSG-CommandandControlSystems.aspx.

[5] K. Ford, “Next Generation of Force level Behaviours: Information Warfare Final Report, SCORE Deliverable D3.4 & D5.3,” Thales, 26 October 2018.

[6] “Email spoofing,” SearchSecurity, [Online]. Available: https://searchsecurity.techtarget.com/definition/email-spoofing.

[7] “All models are wrong,” Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/All_models_are_wrong.

[8] Allied Framework for Modelling & Simulation as a Service, NATO Standard AMSP-02