Human Factors Research and Modelling: Task 4 Investigation of Computer-Generated Forces Modelling of Information Layer Effects

Final Report

Alain Dubreuil
CAE Inc

Prepared By:
CAE Inc
1135 Innovation Drive
Ottawa ON K2K 3G7

Contractor's Document Number: 01DB03
PWGSC Contract Number: W7719-155268/001/TOR
Technical Authority: Mark G. Hazen, Defence Scientist, DRDC – Atlantic Research Centre.

Contract Report
DRDC-RDDC-2016-C105
March 2016

CAE Inc.

1135 Innovation Drive
Ottawa, Ont., K2K 3G7 Canada
Tel: 613-247-0342
Fax: 613-271-0963

HUMAN FACTORS RESEARCH AND MODELLING: TASK 4
INVESTIGATION OF COMPUTER-GENERATED FORCES MODELLING OF INFORMATION LAYER EFFECTS
FINAL REPORT

CONTRACT #: W7719-155268/001/TOR

FOR

DRDC ATLANTIC

9 Grove St., Dartmouth, NS

24 March 2016

Document No. 5870-005 Version 01

APPROVAL SHEET

Document No. 5870-005 Version 01

Document Name: Human Factors Research and Modelling: Task 4
Investigation of CGF Modelling of Information Layer Effects
Final Report

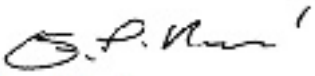
Primary Author

for

Name Alain Dubreuil

Position Senior Military Operations Professional

Reviewer



Name Evan Harris

Position Senior Modelling and Simulation Professional

Approval

Name Damon Gamble

Position Intermediate Project Management Professional

REVISION HISTORY

Revision	Reason for Change	Origin Date
Version 01	Initial document issued.	24 March 2016

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 Background

Many current force level simulations have abstracted the issues of decision-maker knowledge, access to information and communication links, all of which may be vital to the investigation of information warfare issues. A multi-nation workshop will take place in April 2016 to examine how information space effects could be included in new or legacy Computer-Generated Forces (CGF).

CAE was tasked to perform a literature review on the modelling of an information layer and on the simulation of information layer warfare effects (referred to as information layer effects in the remainder of this document). Following the literature review, CAE developed a conceptual architecture for the inclusion of information layer and information layer effects in CGFs. Finally, CAE explored which technologies and research products could be used to implement the proposed conceptual architecture, and how legacy CGFs could be adapted to support the architecture.

1.2 Purpose

The purpose of this document is to provide the results of the literature review, propose a conceptual architecture for the incorporation of information layer effects in CGFs, and report on existing technologies that could support the architecture.

1.3 Document Organization

This document is comprised of the following sections:

- **Section 1** provides introductory and background information;
- **Section 2** lists the references used in this document;
- **Section 3** details the results of the literature review;
- **Section 4** proposes a conceptual architecture;
- **Section 5** discusses issues related to implementation of the conceptual architecture and reports on the technologies that could be included in an implementation;
- **Section 6** provides conclusions and suggestions for future work;
- **Appendix A** defines the acronyms used throughout this document; and

- **Appendix B** lists components of the Coalition Battle Management Language (C-BML) that could be used to report information layer effects.

2 REFERENCES

2.1 References

Abdellaoui N., Taylor A., Parkinson G. (2009), Comparative Analysis of Computer Generated Forces' Artificial Intelligence.

Banks S.B., Stytz M.R. (2013), Using Simulation for Development of Battlefield Intelligent Agents, *18th ICCRTS post conference papers*.

Barreto A.B., Costa P.C.G., Yano E.T. (2013), Using a Semantic Approach to Cyber Impact Assessment.

Bernier M. (2013), MACE Taxonomy.

Blais C. (2011), Application of Coalition Battle Management Language (C-BML) and C-BML Services to Live, Virtual, and Constructive (LVC) Simulation Environments, *Proceedings of the 2011 Winter Simulation Conference, pp 2587-2599*.

Briggs J., Chalmers G., Harris E. (2008), Development of a Network Centric Electronic Warfare (EW) Simulation to Support EW Acquisition.

Brown J.C. (2009), OneSAF Overview and Electronic Warfare Research.

Cioppa T., Lucas T., Sanchez S. (2004), Military Applications of Agent-Based Simulations, *Proceedings of the 2004 Winter Simulation Conference, pp 171-180*.

Evertsz R., Pedrotti M., Busetta P., Acar H. (2009), Populating VBS2 with Realistic Virtual Actors.

Harris E., Graham A., King G., Bieri K. (2008), From DAF to Sim: Simulation Support to Capability Engineering.

Leblanc S.P., Chapman I., Bernier M. (2011), An Overview of Cyber Attack and Computer Network Operations Simulation.

Ling M., Selvestrel M. (2005), An Organisation-Oriented Agents Approach to Modelling Network Centric Warfare.

Malhotra A. (2009), Agent Based Modeling in Defence, *DRDO Science Spectrum, March 2009, pp 60-65*.

ManTech International Corporation (2011), Modeling and Simulation of Cyber Effects in a Degraded Environment, *ITEA 2012 Cyber Conference*.

Marquette D. (2013), Computer Generated Forces & Synthetic Natural Environment Investigation (Current and Projected CGF and SNE Technologies), draft version 2.

Smith R. (2000), Simulating Information Warfare Using the HLA Management Object Model.

Tidhar G., Selvestrel M., Ling M. (2004), Employing Organisation-Oriented Agents to Model Network Centric Warfare.

Van Veldhuizen D.A., Hutson L.J. (1997), A Design Methodology for Domain Independent Computer Generated Forces, *MAICS-97 Proceedings, pp 86-90*.

Wihl L. (2015), Training for the Combined Cyber / Kinetic Battlefield, *MODSIM World 2015*.

Yang A., Curtis N., Abbass H.A., Sarker R., Barlow M. (2005), WISDOM-II: A Network Centric Model for Warfare.

Yen J., Yin J., Ioerger T.R., Miller M.S., Xu D., Volz R.A. (2001), CAST : Collaborative Agents for Simulating Teamwork.

3 LITERATURE REVIEW

3.1 Background and Supporting Information

This section provides background information found in the literature that can be used to support the efforts toward developing information warfare layers in military simulation.

3.1.1 Information Warfare Layer Objectives

In any military mission training environment, one of the goals is to practice gaining a situational awareness (SA) of the environment. "SA is a rapidly changing, ephemeral mental model of an environment that must be assembled over time and continuously updated. Assembling the mental model requires knowledge of the current state of the environment" (Banks, 2013). SA is affected by the information that is being received, including its timing, its quantity (e.g., shortage, overload), its relevance and its validity (e.g., misinformation, erroneous interpretation, sensor error). Properly simulating these aspects of information gathering is important to ensure that the training does not create an expectation for the trainee that information will always be timely, relevant, valid and filtered to show only what is relevant.

The challenges inherent to network centricity also support efforts toward integrating information warfare layers in modern simulations. For example, coordinating bandwidth in a network centric environment is challenging, especially considering that every entity or even two or more components of some entities can become a source or relay of information and Radio Frequency (RF) emissions[1]. This suggests that not every entity is going to be transmitting or receiving information on a continuous basis on a single, worldwide network, but rather that there will be many networks and that any entity will be connected to a limited number of networks. Current CGFs do not support this idea.

The Task Technical Authority (TA), Mark Hazen, provided the following comments[2] on the objectives of information warfare layers:

1. the need for information warfare layers is not only for training purposes, it is also for: concept development of new capabilities, processes, and tactics, techniques and procedures; evaluation of new (or old) warfighting capability; and definition of requirements for new capabilities, all require the ability to include realistic information environments;

2. the term "network" includes non-computer networks; and

3. the concept of an information layer is not limited to the taking in of information and re-transmitting it to others, but the generation of information, which may include the addition of

[1] Wikipedia, URL: https://en.wikipedia.org/wiki/Network-centric_warfare . Accessed on 20 January 2016.
[2] Email Hazen to Dubreuil, 27 January 2016.

biases and/or the selective interpretation of data – even the most well intentioned people add their interpretation of data when relaying it – c.f., Telephone game[3].

3.1.2 Cyber Effects Taxonomy

Bernier (2013) suggests a cyber effect taxonomy which can be used to name and define the effects that different types of cyber attacks may have on a network. A table from Bernier (2013) is reproduced here (Table 3-1):

Table 3-1: Cyber Effect Categories

Effect	Description	Implication
Interruption	An attacker causes an ITI asset to become unusable, unavailable, or lost for some specified period of time. Affects the availability component of the CIA triad.	The ITI or information residing within it is unavailable for a specified period of time and the process will be unusable until recovery from the incident.
Modification	An attacker causes a modification of information, data, protocol, or software. Affects the integrity component of the CIA triad.	The information has been altered and as a result the processes that use this information may fail or produce incorrect results.
Degradation	An attacker causes degradation in the performance of an ITI asset. Affects the availability component of the CIA triad.	The rate of information delivery is decreased resulting in the processes involved becoming slowed down.
Fabrication	An attacker causes false information to be inserted into the system. Affects the integrity component of the CIA triad.	False information has been entered in the system and the process could include the insertion of false operational task that may interfere with legitimate operational tasks.
Interception	An attacker causes or takes advantage of information leaked from the system. Affects the confidentiality component of the CIA triad.	The information and/or the process, either via software or hardware, has been captured by the attacker.

In Table 3-1, the term “CIA triad” refers to the three information characteristics of Confidentiality, Integrity and Availability (CIA). The acronym ITI stands for Information Technology Infrastructure.

The paper also lists the types of attacks that can be carried out.

[3] See Wikipedia: https://en.wikipedia.org/wiki/Chinese_whispers

3.2 Current State

There is limited information available on the state of information warfare simulation, most likely because little work has been done and published in this area. Leblanc (2011) conducted a survey of available literature on the simulation of cyber-attacks and defensive responses to those. All of the systems surveyed were simulating networks of varying sizes with different types of cyber-attacks being conducted on those simulated networks. These systems aimed to either test defensive systems or train network operators and managers (who could be military commanders) on the subject of Computer Network Operations. Only one of the reported simulation programs, the Cyber and Air Joint Effects Demonstration (CAAJED) of 2006, reportedly implemented effects on the war fighting operations. For example, CAAJED operators were asked to degrade associated assets (radar sites, anti-aircraft artillery, etc.) whenever an associated network asset was attacked. Hence, users would be able to observe effects that were consistent with the simulated cyber-attacks.

Effort is ongoing to devise systems that can help to assess the impact of cyber-attacks and determine alternative courses of action. Barreto et al. (2013) provide an overview of several techniques used for this purpose, and propose their own approach to cyber impact assessment. Their approach is based on a mission viewpoint, with the focus being on measuring how the effects generated by a cyber event intervene on the results of tasks performed in a mission. Knowledge bases for task processes, ITI (including the location of vulnerabilities) and enemy behaviour are required as input to the decision-making algorithms. However, the approach is computing-intensive and could not be used in a real-time system.

3.3 Potential Solutions

3.3.1 Agent-Based Modelling and Simulation

3.3.1.1 General

Malhotra (2009) argues that agent-based modelling is well suited to model the dynamically changing networking and C2 structures inherent to the Network Centric Warfare (NCW) theatre. She states:

> *Since NCW is about how members of a team or an organization may better work together with the help of network technology, each member of the team must be aware of the existence of the others in order to be able to model their collaboration and coordination of action. Such team-oriented decision-making skills are an inherent capability of agent-based systems and numerous toolkits are readily available to model this.*
>
> *Agent-based development environments provide an infrastructure specifying communication and interaction protocols, and are typically open and have no centralized designer or top-down control function. Such platforms are widely available commercially nowadays.*

In our opinion, the interactions between individual agents can be dynamically reassigned, a property that can be used to circumvent communication problems that are caused by any factor, for example jamming. This could be built into an agent-based CGF, such that any effects caused by information warfare actions from an enemy formation, whenever the effects are recognized by an affected formation, would cause the affected formation to try to circumvent these effects.

Banks (2013) makes a case for the development of battlefield intelligent agents that could be used to aid military personnel in assessing the value of information, including its security and validity. The authors state:

> *The battlefield entity (represented by an [agent]) will make decisions according to its current beliefs (or perception) of the state of the battlefield. This reasoning behaviour has been borrowed from the theoretical belief-desire-intention (BDI) model of artificial intelligence in which agents have a view of the world (beliefs), certain goals they wish to achieve (desires), and they form plans (intentions) to act on these using their accumulated experience. […] Furthermore, the cyberspace intelligent agent must use its knowledge about the state and security of the cyber battlespace to inform the decision-maker and the real-world intelligent agents about the reliability of the data they are using and thereby constrain their data scope to the data that has the lowest probability of having been tampered or altered.*

In our opinion, the beliefs that an agent has are based on its view of the world, and this is where effective and realistic modelling of inter-communications is valuable. The information that an agent receives about the world must be subject to realistic interferences, which may include such affects as distortion, jamming, interference from the environment, disinformation, conflicting information, timeliness, latency and so on. Furthermore, if agents can be designed to be able of assessing the validity of data, then arguably it should be possible to design agents that can do the opposite; that is, agents could be used to perpetrate attacks such as sending invalid data to the enemy formation. This would require the agents to have a set of beliefs about the adversaries' actions, reactions and ability to assess the validity of received information. The ability to assess the validity of data could also cause an agent to forward only a portion of the received data to other members of its force, or to modify the information based on the agent's own beliefs before using or forwarding it.

3.3.1.2 MANA

Cioppa (2004) summarizes the work to apply agent-based simulations to assess the impact of degraded communications in the US Army's future force. Of interest is the description of how a simulation of jamming was implemented:

> *Agents in MANA [New Zealand's Defence Technology Agency's* Map Aware Non-Uniform Automata simulation *platform] build their perceptions through either their own sensors or over the network. […] MANA does not explicitly propagate electronic transmissions through the environment or model the detailed electronics and signal processing associated with communications equipment. Rather, it lets*

> *the user define which entities are linked together and provides parameters to vary each node or link's capacity, latency, maximum range, queue buffer size, reliability, accuracy, maximum age, and delivery protocol.*
>
> *All of the modeling in this study was done through the input variables—that is, no changes were made to MANA's code. As with most simulation development, there were some things that could not be explicitly modeled. For example, the physics behind the effects of the enemy's jamming was not explicitly simulated. To implicitly model the effects of noise jamming, Lindquist (2004) created fictitious communication nodes through which all Blue forces communicated. Each Blue agent is able to talk through two nodes—one of which captures the communication equipment's inherent capabilities while not under jamming, and another which captures the communication equipment's capability when under jamming. Each of these nodes follows the agents during movement—remaining invisible to the Red force and not affecting the Blue force other than in their role in passing information between agents. When an agent desires to communicate, it will do so through one of the two nodes. If the transmission is not jammed, the "inherent capabilities" node is used. However, when the enemy jams an agent its preferred communications node "runs away" and can't be used, so the agent is forced to use its less capable communications node. This modeling mechanism allowed a variety of levels of communication degradation to be explored.*

The paper also provides findings such as the effect of diminished range, hampered responsiveness in the network, diminished reliability, enemy jamming and so on.

Yang (2005) provided an interesting statement about MANA:

> *MANA introduced the concept of way-points, internal situational awareness (SA) map and event-driven personality changes. The latest version of MANA (released at the end of 2004) concentrated on the model of communication, including the reliability, accuracy, capacity and latency of each communication channel.*

It might be interesting to explore MANA's capabilities in generating and representing information warfare effects. However, no recent articles on MANA have been found.

3.3.1.3 WISDOM-II

Yang (2005) reports about an agent-based implementation called Warfare Intelligent System for Dynamic Optimization of Missions (WISDOM-II). The paper describes the manner in which communications are modelled in the system:

> *Combatant agents can communicate with other agents linked directly to them through the communication network. This communication occurs through a communication channel, which is modelled by noise level, reliability, latency and communication range. The agent may only communicate with the agents within the range of that communication channel. We also adopted a probabilistic model to*

implement the noise level and reliability of a communication channel. Each communication channel has 2 probabilities corresponding to noise level and reliability. At each time step the message can only be transferred from one agent to another agent. The message will permanently be lost if it is older than a number of time steps predefined by the user.

As with MANA, it might be interesting to explore WISDOM II's capabilities in generating or representing information warfare effects, and to determine the status of this system today. However, no recent articles have been found on WISDOM-II.

3.3.1.4 DARNOS

The Dynamic Agents Representation of Networks of Systems (DARNOS) is a modelling and simulation system that is designed to allow Defence analysts to carry out comparative analyses of operations in an NCW context with a special emphasis on the dynamic management and representation of the information environment (Tidhar, 2004). Ling (2005) expands on this description:

DARNOS utilises organisation-oriented agents (called Orgons) to model the organisational structures (Command and Control (C2) and networking) of a networked force. The Orgons capture the organisational knowledge and behaviour, whereas the knowledge and behaviour of single individuals are modelled using single agents called Agons. The reason for using Orgons in DARNOS is that NCW is fundamentally about how members of a team or an organisation may better work together with the help of network technology. Therefore, in an NCW modelling and simulation environment, each member of the team must have awareness or perception of the existence of the others in order to be able to model their collaboration and coordination of action. Such modelling capability is also indispensable for managing the dynamic changes of networking and C2 structures.

Although DARNOS takes an interesting approach to modelling the NCW context, it does not model detailed communication characteristics such as latency, propagation loss, and so on. It concentrates on team behaviour and how organizations interact with each other. There are no papers that have been published that refer to DARNOS since 2008 (Briggs, 2008), (Harris, 2008). The current status of DARNOS is unclear at this time, so getting additional information on how it models communications and whether it lends itself well to the implementation of information warfare layers may be challenging.

3.3.2 Data Representation

3.3.2.1 C2 Base Object Model

Dillman (2009) proposed a Base Object Model (BOM) for networked C2 information. This C2 BOM aims to provide a generalized model of exchanging C2 operational picture information between not only entities, as is usually the case in High Level Architecture (HLA) Federations, but also between systems or components on one or more interconnected networks. The C2

BOM also aimed to facilitate the conversion of specific existing C2 information into C2 BOM format, and provide data traceability information.

3.3.2.2 Information Warfare Using the HLA Management Object Model

Smith (2000) published a paper on simulating Information Warfare using the HLA Management Object Model (MOM). The paper describes concepts and techniques for implementing Information Operations (IO) within a distributed simulation environment supported by the High Level Architecture:

> *The MOM services are specifically intended to allow one federate to "control the functioning of […] individual federates". The MOM provides services that allow any federate to access and influence the information available to any other federate.*

The paper identifies twelve MOM services that could be used, when combined with software models or operator action, to stop, redirect, delay or alter the content of information delivered to a federate. There is a description of how certain attacks could be carried out using the MOM services. For example, for a denial of information attack there would be an IO (Information Operations) federate that would invoke services to blind a federate to an entire class of interactions and/or to change the list of class attributes to which a federate is subscribed. For a delay of delivery "attack", there would have to be a Federation Object Model (FOM) that contains two varying representations of the same object or interaction class. The IO federate would in essence swap a federate's subscription to an object or interaction class with the other representation. The IO federate could then receive the original information, and re-direct it with the desired delay to the federate using the other representation. The paper also provides a description of how to deceive the content, which is using a similar technique as for the delay.

Although this paper is over 15 years old, we assume that newer versions of the HLA standard still support this technique. Also, the paper applies this technique to communications between federates, but this may not work for entities or groups of entities that are generated by the same CGF if the CGF does not rely on HLA messages to exchange information between its entities.

3.3.2.3 C4I FOM

Mostow (1999) reported on efforts undertaken to integrate an Internet Attack Simulator (IAS) in a distributed simulation environment. The paper describes the implementation of various Information Warfare attacks as part of an overall HLA Command, Control, Communications, Computers, and Intelligence (C4I) Federation Object Model (FOM):

> *The FOM, being developed under a separate but related effort, supports a simulation architecture focussed on representing realistic tactical communications including interfaces to real C2 systems. An HLA interface for the IAS is being designed and developed within the context of an existing C4I simulation environment. […] Underlying this simulation environment is a high fidelity real-time model of certain Army communication systems. It provides realistic digital data communications to the simulation and training environment by computing message*

delays and losses in communications based on terrain, network traffic, and radio characteristics.

The system uses a Communication Effects Server to calculate the effects on the communications.

Researching this FOM yields no recent results, so it likely was abandoned or rolled into another project under a different name.

3.4 Papers Not Retained

The following list is a bibliography of papers that were found and considered but not retained for this task. The abstract or a short summary is included for each.

- Bisht S., Malhotra A., Taneja S.B. (2007), Modelling and Simulation of Tactical Team Behaviour:
    - During battlefield simulations, simulated battlefield entities generally represent individualistic behaviour, taking operational order from higher control and executing relevant plans. However, since a complex battlefield scenario typically involves thousands of entities, their coordinated team behaviour should also be considered to make the simulation more realistic. This paper demonstrates the use of intelligent agent-based team behaviour modelling concepts in simulating the armoured tanks in a tactical masking scenario.
- Bisht S., Malhotra A., Taneja S.B. (2004), Using Intelligent Agents to Simulate Battle Tank Tactics:
    - The ability of intelligent agents to model the tactical decision-making behavior of battlefield entities gives an edge over other software techniques because such a problem maps easily into agent based programming. This paper demonstrates the strength of this technology in modelling and simulating the battlefields. As a case study, the tactical and reactive behavior of lower level battlefield entities such as tanks has been modeled using JACK Intelligent Agent framework.
- Brown C. (2015), The Selection of a Common Scenario Scripting Language for UK Royal Navy Combat Systems Integration Assurance:
    - This paper presents a summary of the existing bespoke languages and an assessment of the functionality and capability which these languages support. These are then compared with the Military Simulation Definition Language (MSDL), Coalition Battle Management Language (C-BML) and the evolving Command and Control Simulation (C2SIM) together with an assessment of the expected challenges and benefits of adopting these standards. Where these open standards lack the required features and capability to support the migration from bespoke standards, these are identified.

- Bruzzone A. (~2010), PIOVRA Executive Summary:
    - PIOVRA is Polyfunctional Intelligent Operational Virtual Reality Agents. The project aimed to develop a new generation of CGF able to simulate "intelligent" behavior and was an Italy-France cooperative effort. A PIOVRA CGF aims for consistency of reactions and reproduction of realistic opponent actions and reactions. It demonstrates cooperative and competitive behaviours based on the situation and on current boundary conditions. It runs as part of an HLA federation – a demonstrator was integrated with JTLS on such a federation.
- Edgren M. (2012), Joint M&S Strategy:
    - Powerpoint presentation talking about the need to revamp the M&S efforts from stovepipe efforts into a Joint Training Enterprise Architecture. The strategy looks to give access to M&S efforts and assets on the cloud, using Web 2.0 technologies. The goal is to have, by 2020, Data Services (OOB, terrain, targets, networks, weather) and Modeling Services (air dynamics, sensor modeling, population modeling, simulation behavior) available in the cloud.
- Guo J. (2013), CORA 141 War game Replicator Functional Test Case Final Report:
    - The specific objective of the requirement addressed in this task was to complete a test case demonstrating a capability to produce multiple replications of an interactive war game, such that each replication adequately reflects the real-time decision-making of the human players. This task builds on the work performed in three previous phases.
- Khayari R.E.A., Lotz H.B., Krosta U., Khimeche L., Cuneo X., Remmersmann T. (2015), Practical Use of BML and MSDL Standards for Supporting French German Training:
    - This paper discusses experimentations to assess the applicability of C-BML and MSDL standards to address C2SIM information sharing. The authors highlight the military goals, the operational organizations, the scenario, the technical architectures and the remaining works that are needed for military acceptance.
- Larocque J., Tardioli L. (2012), Discussion Paper – Simulation Integration Version 1.0:
    - This paper provides an overview of some simulation software (Virtual C2 Interface (VCCI), Networks and Comms simulation, etc.). VCCI is a bridge between C2 systems and simulation software (CGFs). It can monitor and control the flow of data between these applications. It supports After Action Review (AAR) and can be integrated with SimSpeak for audio playback. The document identifies requirements for capabilities that are not currently supported (assumed in the LCSS, not necessarily in all products), such as Data Synchronization between C2 or C4ISR systems and Simulations, and improved access to C4ISR data. Appendix A of the document gives a short (one paragraph for each) overview of current simulation products (Abacus, JCATS, VBS2, OneSAF, etc.)

- Logsdon J., Nash D., Barnes M. (2008), OneSAF Capabilities, Architecture and Processes:

    - This is a powerpoint presentation (in PDF format). The slides provide information on OneSAF that may be of interest for the implementation of an information layer, in particular: an architecture for OneSAF; a “composition nomenclature” to specify responsiveness to orders and behavior composition; how activities like intelligence and command and control are represented; and the use of agents to model behavior,along with examples of agents and details about behavior modelling.

- Lovell M., Guo J., Kramer C., Lai G. (2011), Conceptual Study: an AI Driven Wargame Replication Model:

    - The main objectives of this task were twofold. First, using the provided scenario information as a basis, the objective was to document and detail aspects of human decision making that will be critical to replication of this scenario in an AI-driven replicator. Second, an objective was to prototype critical aspects of the AI-driven replicator to start the production of an AI-driven replicator proof of concept.

- Marques H.C., Manso D.F., de Oliveira J.P. (2013), Distributed Simulation with Automated Planning:

    - Reactions to disasters are hampered by lack of effective planning and situation awareness in scenarios where different support teams are working in the same area without coordination. The present work is being conducted to establish a distributed simulation environment, with 3D visualization, to support resource allocation planning and to increase the situation awareness.

- Papasimeon M., Pearce A., Goss S. (2007), The Human Agent Virtual Environment:

    - HAVE is a test bed to explore agent-environment interaction in multi-agent simulation for defence applications. The primary driver of HAVE is to explore representations of virtual environments in which both humans and agents are situated, perceive these environments and undertake meaningful and appropriate actions. HAVE models and simulates a Close Air Support (CAS) mission which involves fighter or strike aircraft providing support to ground troops through the use of air-to-ground weapons. Three important research challenges have been addressed by the work. The first is the implementation of a multi-modal representation of the virtual environment, having multiple, parallel yet consistent representations of the virtual world that were accessible to, and tailored for the different simulation components. The second is the used of labelled annotations in the virtual world which the agents could easily access and interpret. The third is the use of an appropriate architecture for capturing and representing interaction between agents and the environment in which they are situated.

- Sharma V., Sagar A. (2014), An Enhanced Agent Based Simulation Using Selected Viewing Multi-Resolution Modeling:
    - The paper reports on the use of Selected Viewing Multi-Resolution Modeling to design agent-based modeling. The model includes team behavior and their representation for achieving the desired goal. The goal is to help analysis, planning and decision making in the battlefield, decomposing problems to show their hierarchy and executing plans from higher to lower order.
- Shibi-Marr O., Waters M., Mathieson G., Bache L., Tidhar G., Selvestrel M., Ling M. (2006), Developing a Requisite Analytic Trade-Space for Assessing Agile Mission Grouping (Problem Definition):
    - This paper describes the trade-space problems facing defence analysts in both United Kingdom (UK) and Australia, and how they may be addressed through the joint development of the DARNSTORMS model, integrating the Australian DARNOS model and the UK STORM algorithm. Two other related papers focus on theoretical synthesis and implementation issues.
- Shibi-Marr O., Waters M., Mathieson G., Bache L., Tidhar G., Selvestrel M., Ling M. (2006), Developing a Requisite Analytic Trade-Space for Assessing Agile Mission Grouping (Approach):
    - The DARNSTORMS model will integrate the functionality of the Australian Dynamic Agents Representation of Networks of Systems (DARNOS) C2 model with that of the UK Socio-cultural Teamworking for Operational Research Models (STORM) algorithm. It is a joint venture between the two nations to extend the available C2 modelling capability to encompass those social, organisational and cultural issues that are key to any effective, network enabled, multinational coalition operation, a primary deployment mode for our armed forces. In this, it will extend the modelling tradespace available to analysts to cover all Defence Lines Of Development. In particular, it will be able to address the important issues for Coalition C2, Agile Mission Grouping, Training & Experience, Rapid Deployment, Net-enabled C2 and Comprehensive Approach. The current paper deals with those interfacing and other issues that relate directly to the construction and implementation of the DARNSTORMS model itself. In particular, it addresses the approach employed for the calibration of the model parameters and for their uncertainty bounding, within the context of this extended tradespace. It also covers the sensitivity analysis required to assess the varying impact of each of these upon the model output. We present the preliminary results obtained, along with their implications.
- Trott K. (Northrop Grumman) (2003), C4ISR Modelling and Simulation Using JSAF:
    - The objective of the discussed project was to establish a flexible C4ISR Modeling & Simulation framework based on JSAF software.

- Trott K. (Northrop Grumman) (2006), Simulation Development for Dynamic Awareness and Prediction II:
    - The objective of the project was to develop a closed-loop simulation environment in which detailed mission plans can be developed, used as input to a set of distributed simulations, and executed within the simulation environment. These simulations provide feedback to prototype C4ISR systems in the form of mission status reports, sensor tracks, and other ISR mission results reports, which can be used to maintain situation awareness and to dynamically adjust mission plans in response to events." The authors tried to capture video showing the Dynamic NCW concept (forces reacting to actions taken by enemies and detected by an Unmanned Air Vehicle (UAV)).
- Unrau D. (2012), CORA Task 129 Final Report:
    - The goal of the project was to define a decision making schema for blue and red entities. The schema was to parameterize a realistic range of possible courses of action likely to be considered by human-in-the-loop players in a wargame context. Project also developed a simplified proof-of-concept AI-driven wargame replication system that implements the decision-making schema. Also, a fitness test application was created to test the validity of non-AI wargame replications in an automated fashion. Finally, requirements were defined for the replication engine.

4 CONCEPTUAL ARCHITECTURE

This section presents a conceptual architecture for a CGF that includes the movement of information and the information layer effects that can be applied against the channels employed to move the information amongst simulation objects. First, a definition of the term *information layer* is given. This is followed by a discussion of the problem that the conceptual architecture attempts to solve. Finally the conceptual architecture is detailed.

4.1 Information Layer Definition

During a teleconference held on 26 January 2016 and attended by the TA, the definition of an information layer was discussed. It was concluded that:

1. The information layer is the structure that allows the modelling of information content, its modification and movement. The structure includes an architecture and data formats.

2. The information layer should allow for:

    a. the concepts that information is generated, stored, requested, modified and consumed by Live, Virtual and Constructive (LVC) entities;

    b. time issues such as latency in the movement of information; and

    c. the concept that an information channel may introduce errors in the information transmitted.

3. The information layer does not specify how an entity generates, consumes or modifies information.

4.2 Problem-Space Discussion

4.2.1 High-Level View of the Problem

Figure 4-1 depicts at a very high level the problem that the information layer attempts to solve in simulated environments. The figure shows that a simulation contains many entities that can be live, constructive or virtual. From the point of view of a CGF, the entities can be home-grown (i.e., generated and controlled by the CGF), but they can also come from other sources through a distributed network protocol such as Distributed Interactive Simulation (DIS) or HLA. The entire simulation may run inside a single CGF, or it may be shared across many individual participants in a distributed simulation. All of the entities exchange information amongst themselves and can gain information from various non-entity sources like sensors, internet, telephone, face-to-face verbal, and so on. An entity may receive information in a passive manner from other entities and from sensors, but it may also gather information in a proactive manner through requests for information, internet searches, remote sensor activation and so on. The environment affects some information channels, or *mediums*, in various ways. For

example, terrain may block or interfere with certain types of communications, activity on a network may interfere with a transmission, and weather may cause interference or reduce the ranges. Hackers or enemy forces may also attack various networks using various methods such as jamming, denial of service, spoofing and so on.

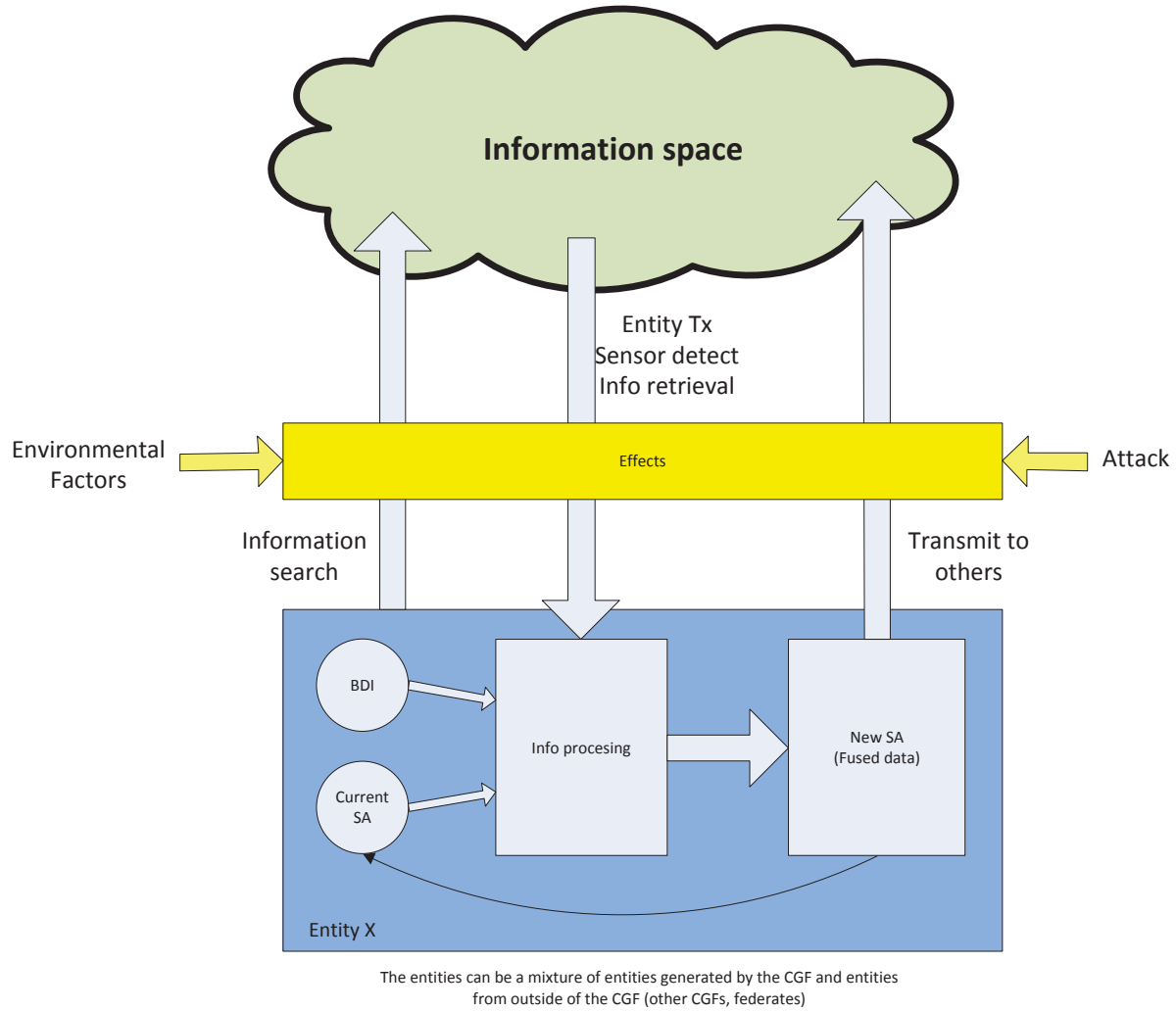


Figure 4-1: High-Level View of Information Layer Problem.

The *Entity X* box in Figure 4-1 shows that information from a variety of sources is received and processed by the entity. The beliefs, desires and intentions of the entity along with its current understanding of the situation affect this information processing activity, which eventually outputs a new situational awareness picture. The entity may transmit information to other entities based on that new situational awareness, and this information may or may not differ from the information that was received by the entity.

The information layer represents and simulates the yellow box in the figure, i.e., it applies the effects of the natural and human-generated interferences to the information exchanged between entities or pulled from non-entity sources. It also models the dynamic aspects of information, i.e., the fact that information may be requested from other entities or searched for and retrieved, and then modified by an entity before it is transmitted or forwarded to other entities. The entities may modify the information for a variety of reasons, including omission, transcription errors, filtering and overt modification.

The definition in paragraph 4.1 specifies "[…] structure that allows the modelling of information content, modification and movement". In a distributed simulation context, current distributed simulation protocols allow for the movement of information using standardized messages where the form is predefined but not necessarily the contents. The protocols allow for the periodic or occasional update (modification) to that information. Where the current protocols and models that use them to send and receive information fall short is with the application of transmission latencies and errors, and with the application of cyber effects to the information transfers. The rest of this section offers possible solutions or avenues of research to solve these shortcomings.

4.2.2 Information Sources and Mediums

The information layer can be seen as a medium through which all information being exchanged between entities flows. Information being exchanged can come from a variety of sources, going through a variety of mediums. Table 4-1 gives an overview of sources and their associated mediums, although this is not meant to be a complete list.

Table 4-1: Information sources and mediums.

Information source	Medium(s)
Local Area Network/Wide Area Network/Internet data services and storage sites	Satellite, telephone land line, coaxial cable, radio waves ("wireless"), network
Radio communications	Radio waves (HF, UHF, VHF), satellite
Tactical data link	Radio waves
Telephone calls	Satellite, telephone land line, coaxial cable, fibre optic, radio waves ("wireless")
Instant messages	Satellite, radio waves ("wireless")
Facsimile	Satellite, land line, coaxial cable, radio waves ("wireless")
Teletype, telegraph messages	Radio waves, telephone land lines
Remote sensors (e.g., UAVs)	Radio waves, satellite
News feeds, televised news programs, commercial radio channel news programs	Network, satellite, telephone land line, coaxial cable, fibre optic, radio waves ("wireless")

Information source	Medium(s)
Intelligence reports	Obtained from or reported to others via network, satellite, telephone land line, coaxial cable, fibre optic, radio waves
Visual/sensory observation reports, signals	Reported to others via network, satellite, telephone land line, coaxial cable, fibre optic, radio waves
Reasoning, i.e., derived from other information	Reported to others via network, satellite, telephone land line, coaxial cable, fibre optic, radio waves
Direct verbal, face-to-face conversation	Reported to others via network, satellite, telephone land line, coaxial cable, fibre optic, wireless, radio waves
Submarine communications	Acoustics waves, radio waves, lasers

Commonality in the table clearly comes out with respect to the mediums. "Information layer effects" are those human-generated or environment-based effects that can be applied to an information transfer medium and that affect the timing, quantity, relevance and/or validity of the information transfer. If one were to simulate information layer effects, a starting point could be to identify which effects apply to each medium. To take it one step further, the usage of each medium by different sources of information is not necessarily the same. For example, a merchant ship communicating with another ship on a radio will do so in an unencrypted manner, whereas a military ship communicating with another will likely use encryption and also a frequency hopping mechanism. The former is easier to tap, spoof or jam than the latter, by several orders of magnitude. Hence, the effects that may be applied to a medium may not necessarily affect each user with the same severity.

4.2.3 Information Layer Effects

Implementing information layer effects and its causes can be done at varying levels of fidelity. When implementing information layer effects, it will not always be important or necessary to simulate the *cause* of the effect. For example, if attempting to simulate a Denial of Service attack on a network server, the attack itself is not useful unless the aim of the simulation is to train network technicians to recognize and counter the attack. What is important is to make the server, or at least the service that the server would provide in real life, unavailable to the (real or simulated) users of the server.

In some cases, it may be advantageous to simulate the source of the attack. For example, in the case of jamming it may be important to simulate the jamming source as its position has an effect on the area that is affected by the jamming attack and also because one of the counteractions may be to attempt the localisation and destruction of the source.

The effects that should be supported by the proposed architecture fall in two categories: human initiated effects and environmental effects. Human initiated effects are human initiated actions that aim to disrupt a network, such as interdiction operations, cyber attacks, influence operations and spying. Environmental effects are nature-based or human initiated actions that cause the environment in which an information medium operates to degrade or block the information transfer. Table 4-2 gives an overview of the information layer effects and their associated category[4]. The table also indicates which transmission mediums can be affected by each effect.

Table 4-2: Information Layer Effects

Effect	Category	Description/Implication	Affected Mediums
Interruption	Human	An attacker causes an ITI asset to become unusable, unavailable, or lost for some specified period of time. The ITI or information residing within it is unavailable for a specified period of time and the process will be unusable until recovery from the incident.	Network
Modification	Human	An attacker causes a modification of information, data, protocol, or software. The information has been altered and as a result the processes that use this information may fail or produce incorrect results.	Network
Degradation	Human	An attacker causes degradation in the performance of an ITI asset. The rate of information delivery is decreased resulting in the processes involved becoming slowed down.	Network, telephone land line, coaxial cable
Fabrication	Human	An attacker causes false information to be inserted into the system. The process could include the insertion of false operational task that may interfere with legitimate operational tasks.	Network, telephone land line, coaxial cable, radio waves, fibre optic, satellite
Interception	Human	An attacker causes or takes advantage of information leaked from the system. The information and/or the process is available to the opposing force and could be used against own force.	Network, telephone land line, radio waves, acoustic waves, fibre optic, coaxial cable, satellite
Interference	Environmental	Environmental factors or jamming initiatives interfere with the communications, affecting the intelligibility of the information.	Radio waves, satellite, telephone land lines, acoustic waves, laser

[4] The Human category effects are from Bernier (2013), where they are referred to as Cyber effects, as reported in section 3.1.2.

Effect	Category	Description/Implication	Affected Mediums
Blockage	Environmental	Terrain features block the communications.	Radio waves, laser, satellite, acoustic waves
Propagation loss	Environmental	The distance between two entities, possibly combined with disrupting factors, causes an emitter to be out of range from an intended receiver.	Radio waves, acoustic waves, coaxial cable, laser

Any proposed architecture to implement information layer effects should strive to support all of the effects mentioned in Table 4-2.

4.3 Proposed Architecture

4.3.1 Assumptions

This paragraph identifies assumptions that guide the development of a proposed architecture. Four assumptions have been identified and are further elaborated upon:

1. Independent control of information layer effects.
2. Universality of the proposed architecture.
3. Information movement in CGFs is internal.
4. Networks must be visible.

4.3.1.1 Independent Control of Information Layer Effects

Rogers (2000) states:

> *"The very character of real Information Operations (IO)[5] is that it enters the battlefield independent of those that it targets and without requiring their compliance to be effective. IO attempts to stand between a combat object and its access to information. The purpose is to deny, delay, or distort the information accessible to the combat object. A simulation technique that could place the IO simulation conceptually between the combat object and its information source would be ideal. It is impractical or impossible for the IO software to be inserted into a federation such that it is physically between the combat object and its information flow. Therefore, we are searching for ways to model IO such that it is conceptually in that position for any combat object in the federation."*

[5] Rogers (2000) defines Information Operations as "various techniques for controlling or influencing the knowledge, perception, judgement, and decision making of an enemy force."

Because IO (or information warfare) stands in-between combat objects and their access to information, it is reasonable to assume that any implementation of information layer effects should be independent from the combat objects. The combat objects will be affected by the information layer effects but will not know in most cases where the effect comes from. The independent information layer effects implementation must have a representation of the communication networks that exist in the simulation, so as to be able to apply effects to specific networks. How the information layer effects implementation learns about the existence of each communication network inside a simulation is a question that must be answered as a product of further research and development.

4.3.1.2 Universality of the Proposed Architecture

In this report, the proposed conceptual architecture is independent of whether it will be implemented within a single process on a single computing device, or within a fully distributed simulation. Hence, technologies such as DIS and HLA are ignored at the level of the architecture presented.

4.3.1.3 Information Movement in CGF is Internal

CGFs manage many combat objects such as platforms, projectiles, humans, animals and so on. The information being passed between a CGF's objects and an independent simulator will be through a distributed protocol such as DIS or HLA. However, information passed between two objects generated and managed by the same CGF is assumed to be moved internally to the CGF application. The CGF must be able to propagate any information layer effect that is generated outside of the CGF to its internal information movement. For example, if an information layer implementation applies a jamming effect to a range of radio frequencies, then the CGF internally must block all communications that are taking place on those jammed frequencies between the entities that it controls.

4.3.1.4 Networks Must be Visible

To be able to apply information layer effects, the communication networks that exist in the simulation must be known and visible to the mechanism used to apply the effects. The parameters of each network (type, encryption status, protocol used, etc.) must be known to ensure that the effect that is applied to the network is suitable.

4.3.2 Conceptual Architecture Proposal

This paragraph describes a conceptual architecture to support an information layer and information layer effects. Different aspects of the architecture are presented in separate sections:

- The *logical networks view* section presents the architecture centered on the logical networks that carry the information across a simulated environment.

- The *interface to external communications* section provides details on the conceptual architecture interfaces with external applications through external communication networks.

- The *entity model* section concentrates on the architecture of a single entity that supports realistic behaviours in an environment where information layer effects exist.

- The *ILEC model* section details an architecture for an Information Layer Effects Controller (ILEC) that allows the imposition of information layer effects on a simulation environment.

4.3.2.1 Logical Networks View

Based on the first assumption that the implementation of information layer effects should be independent from the combat objects, a proposed architecture includes one or more stand-alone controllers of the effects. These controllers have a view of the logical networks and are able to apply effects to them.

Figure 4-2 shows an ILEC that has knowledge of and a connection to a number of logical networks. The figure also shows an example of the application of an information layer effect on one of the logical networks. The ILEC is independent from the client models, the client models representing any object operating in the simulation environment. The effects that the ILEC applies to the networks can be influenced by environment parameters such as the weather and under direction from effects parameters that are controlled externally, perhaps by an operator through a Graphical User Interface (GUI). The information movement between the client models goes through a communication networks infrastructure that may include one or more of the communication mediums from Table 4-1. The ILEC applies an effect to one of the logical networks, causing two client models (numbers 3 and 4) to be unable to communicate with each other, as seen in the breakage in the red connection line in the figure.

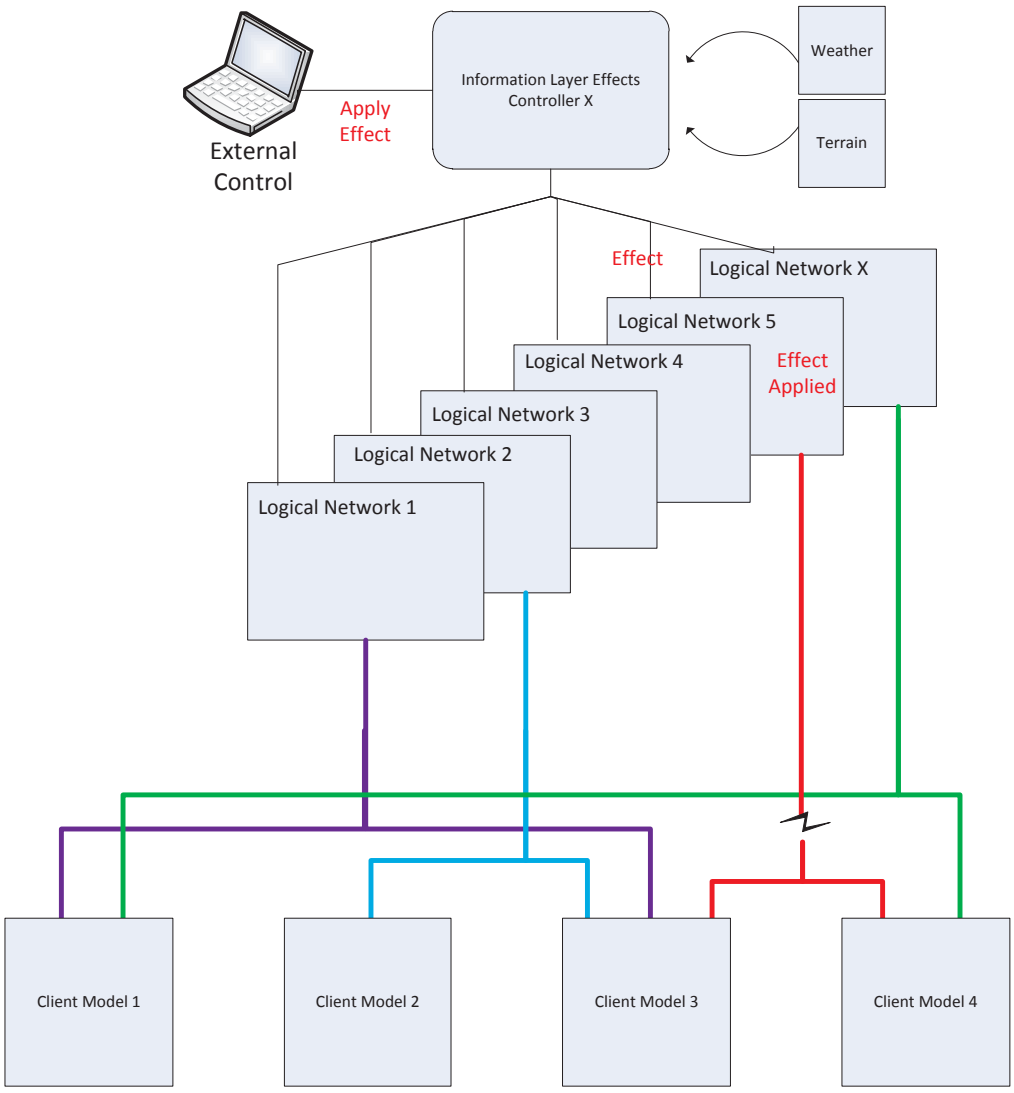


Figure 4-2: Logical Networks View of the Conceptual Architecture.

4.3.2.2 Interface to External Communications

CGFs manage and control a variety of objects while also optionally interacting with externally-managed objects via an external interface or Application Programming Interface (API). They keep track of which force each object belongs to (blue, red or neutral) and use artificial intelligence or some other methods to attempt to give realistic behaviours to the objects that they control based on the object's force, state, tasks, encounters and so on. Information passing between the objects in existing CGFs is often limited to passing information to one or all objects of the same force or team without regard to effects such as terrain blocking and propagation loss or organisational hierarchy. Most existing CGFs also offer the possibility of sending messages from one entity to another but, again, typically with no degradation effect.

However, existing CGFs are generally reasonably proficient at applying terrain blocking and range limits to sensors.

In the proposed conceptual architecture, the application of information layer effects is loosely coupled from the other components of the simulation. There may be several ILECs operating in a simulation environment, and inside a single component of a simulation there may be zero to many ILECs, depending on the needs of the component and on the design of the ILECs. In the case of a CGF that manages several combat objects communicating with one another, the CGF must be able to apply any active information layer effect to all of the communications that take place over the affected information channel, whether the communication takes place between entities that are managed by the CGF (i.e., internally to the CGF) or between CGF entities and external entities (i.e., through an external interface).

To be able to apply information layer effects to the information passing internally to a CGF, the architecture of the CGF should have a representation of the external simulation communication networks that exist in the full simulation environment. Any effect applied to the external simulation communication networks needs to be reflected in the CGF's representation of these networks. Conversely, any effect applied by an ILEC that operates inside of the CGF's architecture needs to be propagated to the simulation communication networks that are external to the CGF. Figure 4-3 depicts these concepts.

In Figure 4-3, it can be seen that the CGF manages a number of combat objects (shown as entities) which exist as part of a dynamic organizational structure representation also managed by the CGF. This dynamic organizational structure allows the CGF to manage command and control relationships, to define for each object which information exchange links it has with other simulation objects, and to form and modify teams dynamically to respond to evolving mission objectives. The CGF maintains a communication networks representation which is synchronized with the external simulation communication networks instance. When an information layer effect is applied to an externally modelled communication network, the CGF receives that information and applies the effects to its own representation of that communication network. This is done to ensure that any information passing that is attempted between two CGF objects, such as the one shown in purple in the figure, is subject to any effect that may be applied on the communication network over which the information is passed.

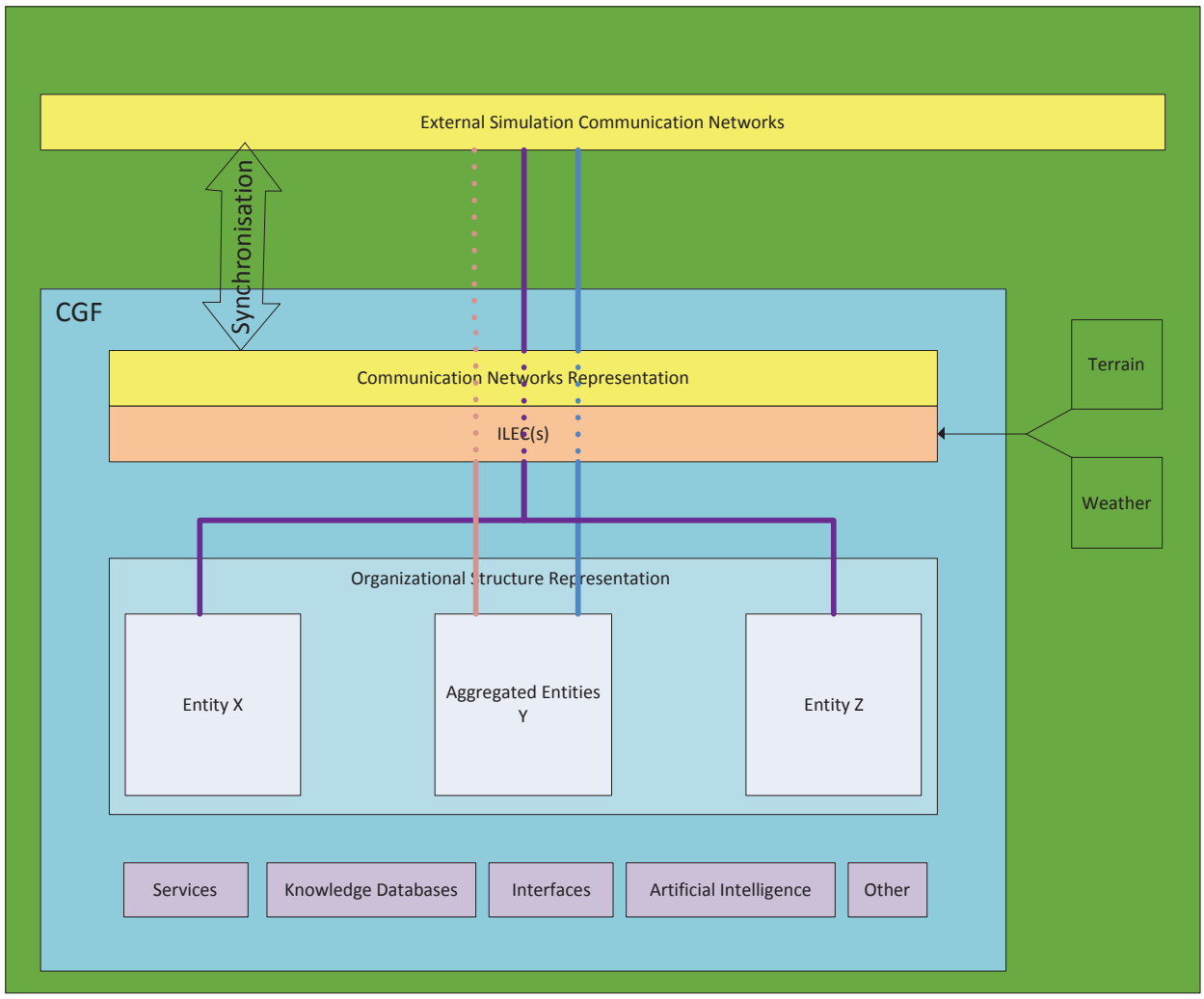


Figure 4-3: Interface to External Communications

The ILEC component in the figure can apply information layer effects to the representation of the external simulation communication networks. When any effect is applied, the effect is propagated to the external simulation communication networks so that objects that are external to the CGF and that use the affected communication network are also subjected to the applied effect. All CGF communications and those externally transmitted from or received by the CGF go through the ILEC component. When an information layer effect is active, the ILEC will apply the effect to any communication that goes through the affected communication network. For example, if the communication is a radio transmission over a frequency that is jammed, then the ILEC will intercept the message and garble its payload.

The figure shows three individually coloured communication lines. The purple line represents a communication line between entity X and entity Z, but also to the external simulation communication network. The blue line represents a communication line between the

Aggregated Entities Z and the external simulation communication network. Finally, the orange line shows a line that goes only to the CGF's representation of the external communication networks; this is meant to represent information passing amongst the aggregated entities. The dotted orange line has a special purpose: even though the communications between the aggregated entities occur within the CGF, the existence of the network connecting the entities to one another must be known to the rest of the external simulation. This is done to allow objects that are external to the CGF to connect to the network if they have the means to do so. It also allows an ILEC that exists elsewhere in the external simulated environment, for example in another CGF, to apply effects to the network.

At the bottom of Figure 4-3 are pink-coloured boxes that represent some of the other elements that may be part of a CGF architecture. In relation to information layer effects, the *Services* may offer algorithms to calculate communication ranges and objects' inclusion in or exclusion from the communication range, terrain blockage affecting communications, and other similar calculations. The *Artificial Intelligence* may be used in concert with the *Knowledge Databases* to reorganize the organizational structures if a mission is severely hampered by the information layer effects, or to identify alternative means to pass the information from one object to another when the communication link between them is severed. The interfaces may be used to control some of the parameters affecting the communication networks linking objects together. How these different elements are implemented in specific technologies is subject to ongoing research as reported in section 3.

4.3.2.3 Entity Model

Much research has been carried out over the last two decades to develop entity models that behave as closely as possible to real entities in similar situations. Many different approaches have been explored, which have led to a variety of agent-based models that attempt to replicate human reasoning and behaviour in specific situations. On the other hand, no single approach has yielded a single general solution that solves a large array of situations.

The DARNOS project (refer to paragraph 3.3.1.4) is one approach that showed promise as a basis for supporting the implementation of information layer effects. Although the papers published about DARNOS mention that information layer effects may be applied, no details are given as to how they were implemented. One of the interesting aspects in the DARNOS approach is the representation of a "C2 grid" and of an "Information grid" which allow the capture of the organizational structure and who the entity being modelled can exchange information with. Modelling these elements allows a more flexible response to the information layer effects.

The conceptual architecture for an entity model is shown in Figure 4-4. The architecture has been inspired largely by a combination of the DARNOS model (Tidhar, 2004) and the concepts presented in the Van Veldhuizen (1997) paper. The architecture is composed of three grids: the cognitive, the physical and the relationships grids.

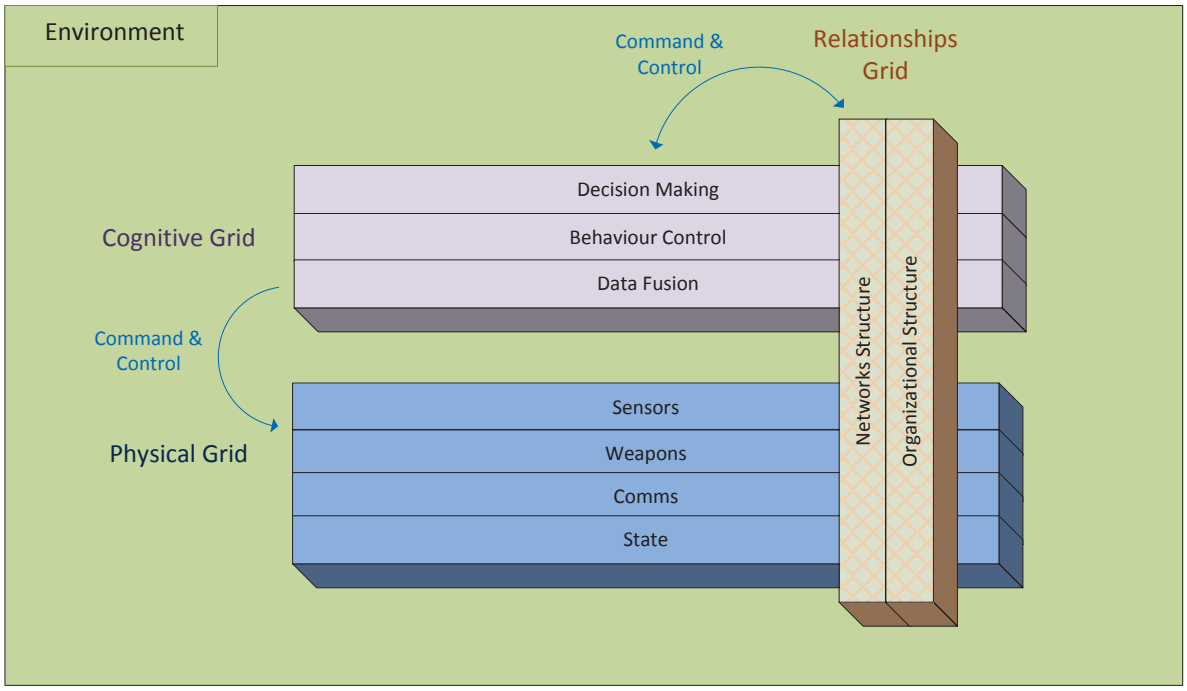


Figure 4-4: Entity Conceptual Architecture

The cognitive grid is the centre of control of the entity. It is composed of a decision making component to decide on the next actions, a behaviour control component to control the movement and reactions of the entity, and a data fusion component to amalgamate the incoming information with the information already acquired and update the situational awareness picture. The cognitive grid also receives orders from superiors. These orders may cause the cognitive component to issue control commands to the physical grid (e.g., to point a sensor in a specific direction or engage a weapon towards a target) and to issue commands to other entities that it controls in accordance with the organizational structure.

The physical grid models the interactions with the physical environment. Its Sensors component models the various sensors that the entity uses to detect and track other objects present in the environment. Its Weapons component controls the weapons with which the entity can engage opposing forces – these weapons may be lethal (e.g., a missile) or non-lethal (e.g., a jammer). Its Comms component models the information sharing equipment that the entity has, such as radios, internet connections, mobile phones and so on. Finally, its State component tracks the status of the entity and its equipment. The State component feeds the cognitive grid with information that can be used for behaviour control and decision making in particular. For example, the damage state of the entity may prevent a specific action that would otherwise be possible if the entity was healthy. The physical grid receives commands and controls from the cognitive grid.

The relationships grid models the information sharing relationships and hierarchical relationships of the entity. Its organizational structure component tracks the C2 relationship and

team composition of the entity, i.e., who can it receive commands from, who can it gives orders to and who is part of its team for the current task. The networks structure component keeps track of who the entity can share information with and over which communication medium(s). External C2 and situational awareness information received by or transmitted from the entity is vetted through the relationships grid to ensure that it comes from or goes to a legitimate entity. It is important to note that the existence of an information sharing relationship between the entity and some other object does not guarantee a connection. A connection will only be possible if the physical grid's Comms component contains a physical communication link that is healthy and active.

Some of the components of the entity conceptual architecture may be omitted, depending on the type of entity that is being implemented. For example, the *sensors* component would be omitted if the entity being implemented does not have any sensors. Also, the level of complexity of a component may differ significantly from one entity to another. For example, an "intelligence analyst" entity might have a much more complex *data fusion* component than a soldier entrenched in the battlefield.

4.3.2.4 ILEC Model

The ILEC's purpose is to monitor the logical networks that exist in a simulation and apply information layer effects to selected logical networks. The ILEC could be a single all-encompassing application or it could be a collection of applications, each responsible for applying specific effects.

Figure 4-5 shows a proposed architecture for the ILEC. At the base of the architecture is a networks interface layer whose purpose is to monitor information movement, maintain the status of the logical networks (i.e., whether or not effects are applied to it), and output information layer effects to the logical networks. That layer would also publish information about the status of the logical networks so that other applications (other ILECs, CGFs, simulators, test equipment…) can apply any controls that they have been programmed to apply.

The information layer effects services layer is where the processing to apply information layer effects takes place. This layer interacts with the environment interface layer to take into consideration the terrain, weather and environmental interference[6] where appropriate. It also takes input from the control layer to obtain the parameters that determine which effects to apply, if any. Finally, it takes into consideration information security (i.e., the resiliency and security measures that have been applied to protect the information against human initiated and environmental interference).

[6] An example of environmental interference is the use of a range of frequencies by taxi cabs, which cause these frequencies to be severely degraded for military usage. It is not an attack. This is prominent close to shorelines near larger cities.

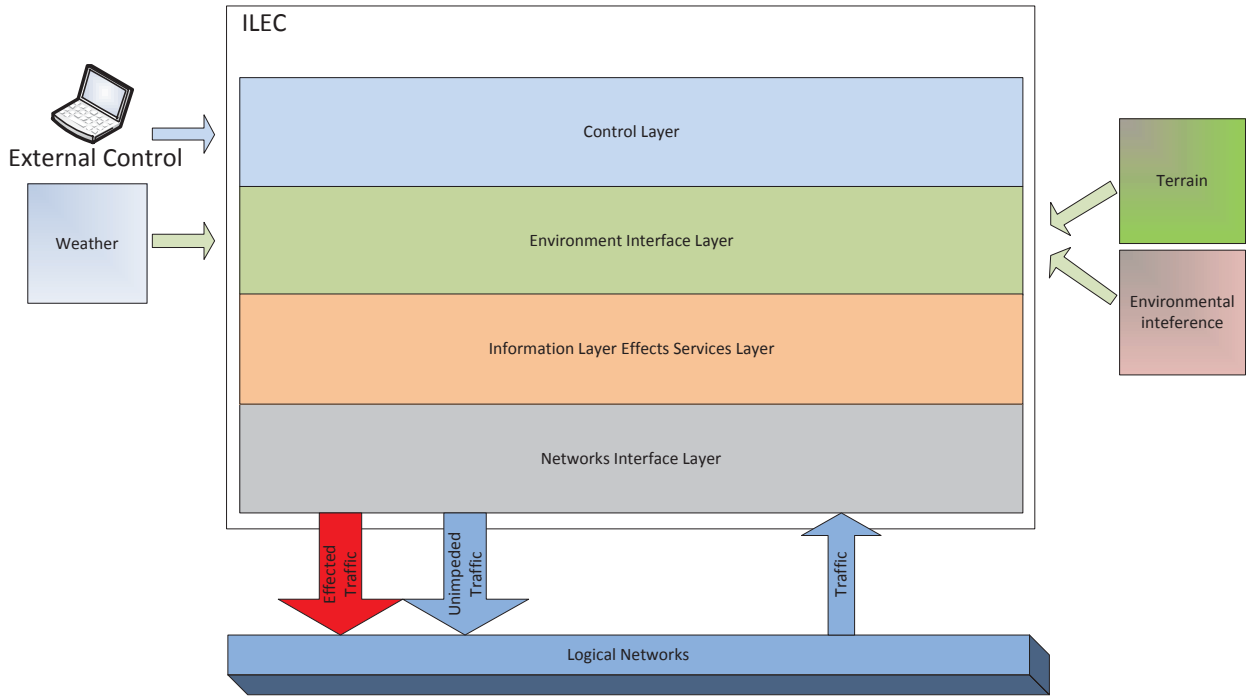


Figure 4-5: Possible ILEC Architecture

The environment interface layer interacts with the information layer effects services layer to provide terrain, weather and environmental interference data that may affect information movement. It may carry out calculations on behalf of the information layer effects services layer (e.g., calculating line of sight or terrain obstructions).

The control layer provides the necessary hooks to allow external control of the interface layer effects. This control could take several forms, including a GUI, a set of configuration files, artificial intelligence or input from automated test/experiment equipment. Control may also be applied by the control layer without input from external components. For example, there could be a set of pre-programmed logical functions that apply effects based on the occurrence of specific conditions.

5 IMPLEMENTATION ISSUES AND TECHNOLOGICAL SOLUTIONS

This section discusses how the conceptual architecture for an information layer may be implemented in concrete applications, processes and/or components. Generic implementation issues are discussed first, followed by a review of a selection of technological solutions that could assist the implementation. A short discussion on adapting legacy CGFs to support the architecture follows before concluding the section with an interim solution proposal.

5.1 Implementation Issues

5.1.1 Discussion

When considering how the conceptual architecture could be implemented, a few issues emerge. The first issue is the implementation of the ILEC. Conceptually, having an ILEC implemented inside a CGF application works but in practice it may not be ideal. It may be better to have the ILEC as a standalone application (or set of applications) that integrates with the set of logical communication networks that is established for the simulation. This is depicted in Figure 5-1.

In this case, the CGF does not need an internal representation of the simulation communications networks. Rather, all communications occurring between entities go through the simulation communication networks and the ILEC. This applies to communications that are between entities inside the CGF, and to communications between entities that are controlled by different applications. The ILEC will let a communication go through unaffected if no information layer effect is applied to the relevant network, but will affect the communication if an information layer effect is applied to the network. Another option would be to have an ILEC instance connected to each logical network to which an information layer effect is to be applied, but not to the unaffected logical networks. The main advantage of having ILEC(s) as standalone applications is that many legacy applications would not require any significant changes to be affected by the information layer effects. The main exception would be CGFs that manage several entities, as the communication methods in-between the entities would have to change. The main disadvantage of having ILEC(s) as standalone applications is that it may increase network traffic significantly as communications that would normally be kept inside the CGF(s) are now published to the full simulation.

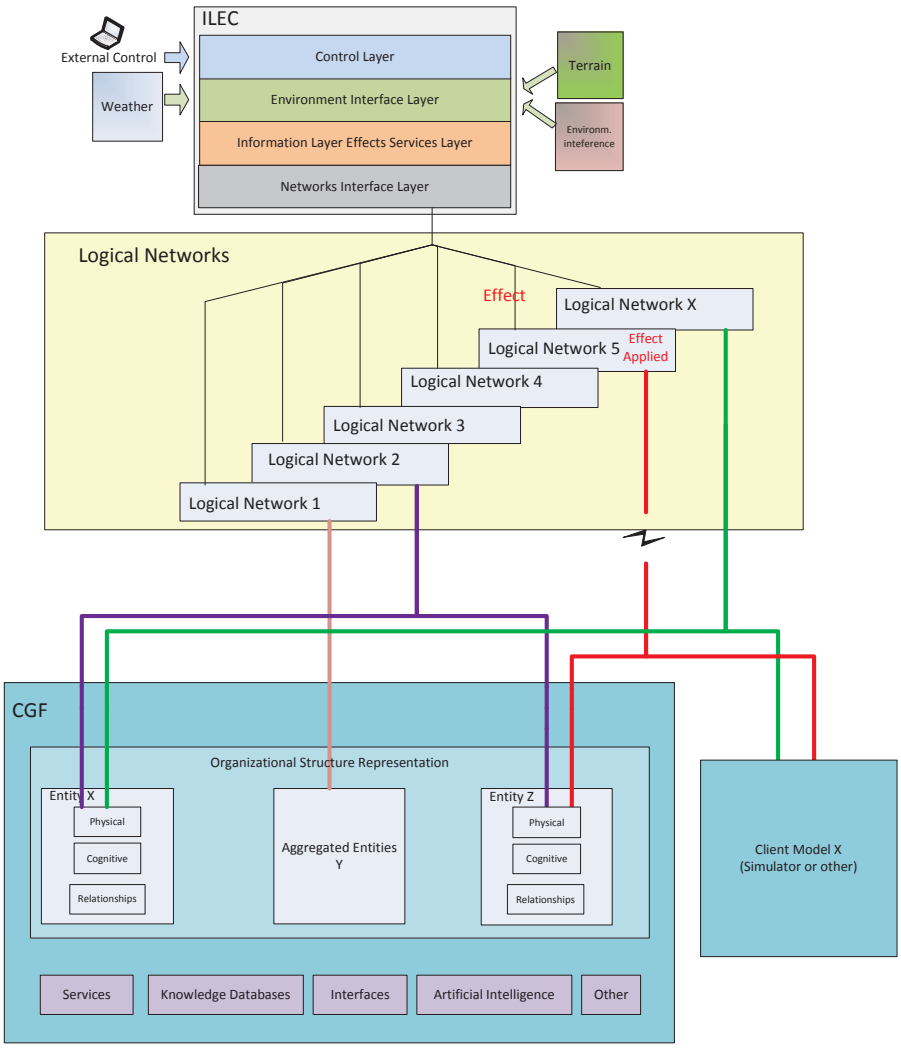


Figure 5-1: ILEC as Standalone Application

If network traffic is assessed as a significant problem, then the option to have the ILEC(s) inside the CGF is a possibility. However, it would likely entail that in a distributed simulation environment, all participating applications that have communication capabilities would also have one or more ILEC instances. Applications that do not instantiate an ILEC could have successful, unaffected communications when in fact their communications should be affected by an information layer effect. This approach is depicted in Figure 5-2, which shows that both the CGF and the client model have one or more ILEC instantiated. Both are synchronized via some information exchange mechanism so that both are aware of what networks exist and what information layer effects are being applied. Both also take the terrain and weather into consideration for the application of information layer effects.

In the case of the CGF of Figure 5-2, it has an internal representation of the logical networks that exist in the simulation. Communications between the entities that are controlled by the CGF are only published to the simulation's logical networks if at least one external application connects to the logical network used for the communication; otherwise, the communications are not published. Even though the communications are not published, there may be a need to publish the fact that communications are active on that logical network. This would allow an external application to be aware of the existence of traffic and offer the possibility to connect to that network and apply an effect such as tapping or spoofing. If the logical network is not active, then an external application would normally have no need to apply an effect to it, except for specific cases like jamming (to prevent usage of the jammed frequencies).

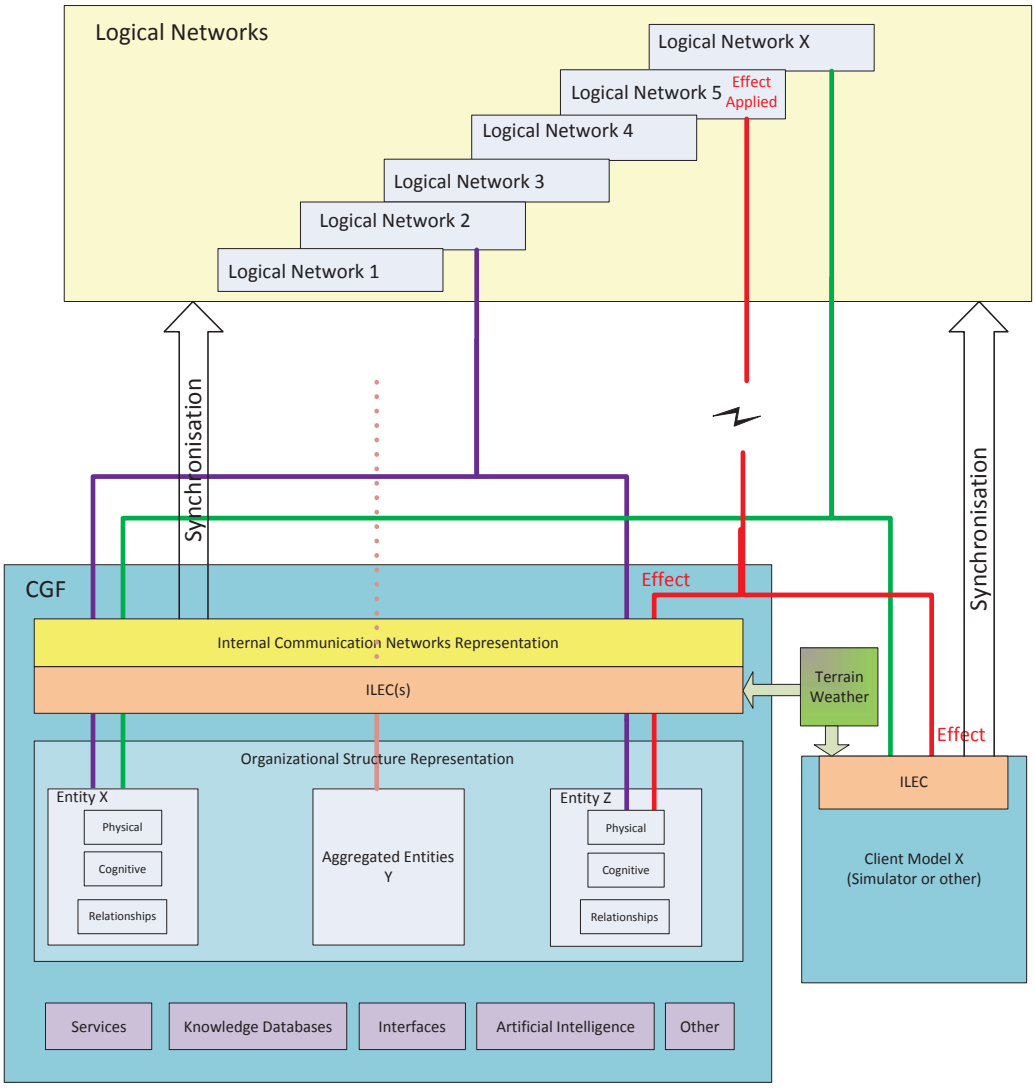


Figure 5-2: ILECs as Part of Individual Applications

Other implementation approaches are also possible. The implementation of the ILEC itself could be treated as a "third-party product": any organisation could design an ILEC implementation which could then be integrated in any client model. What would be required is a standard detailing how the information about the information layer effects and the logical networks that exist in a simulation is published and shared between the applications. That information is not published in current simulations, so effort would be required to develop a standard to regulate how that information is exchanged.

There is also a need to develop an entity structure that can react to information layer effects in a way that is representative of real world reactions/adaptation to similar effects. The cognitive grid of the entity conceptual architecture (paragraph 4.3.2.3) comes into play for this part of the effort, with the relationships grid playing an important role as well.

One additional issue with the implementation of information layer effects is the influence of terrain and weather. One of the problems in current distributed simulations is the lack of uniformity in the representation of terrain and of weather. Each client model normally has its own terrain database whose fidelity depends on the source of the data used to build the database and also on the scenario requirements and on the system requirements and capabilities. This misalignment can create situations where one application concludes that the communication between two entities is possible while another application concludes the opposite. How to resolve these situations would have to be explored. One possibility would be to use a brokering system, for example adopting the least favourable conclusion (i.e., the communication is not feasible). Another possibility would be to ensure that all participating applications in a simulation are using the same terrain source data—the Royal Canadian Air Force is moving in that direction with its Virtual Battlespace which will serve terrain and weather data from a central location. However it remains to be seen if each client model's technical limitations will prevent this centralized distribution of terrain and weather data from effectively rendering a uniform terrain and weather representation across all simulation applications. It may be necessary to extend, revise or update the capabilities of client models.

5.1.2 Data Requirements

To implement a reusable and permanent solution for information layer effects, recognized data structures will be required. As a starting point for discussion, a preliminary list of published data could include:

- **Logical Networks Structure**: A description of each logical network structure, to include at least:
    - ID: An identification string or number for the network;
    - Type: The type of medium in use (radio waves, computer network, telephone land line, etc.);
    - Encryption status: Whether the network is encrypted or not, and possibly the strength of encryption;

  - Frequency range: This may be a single frequency, or a range of frequencies. Applies only to specific types of mediums;
  - Attack status: Whether the network is under attack or not, and the type of attack;
  - Range attenuation: The percentage of attenuation imposed on the maximum range of a transmitter on the network, due to environmental factors. The maximum range is a function of the transmitter in most cases where weather is a factor. This value would reduce the maximum range of a transmission as opposed to perfect conditions; and
  - Propagation loss: The percentage of the maximum range at which the propagation loss should start.

- **Information Layer Effects Parameters**: A description of information layer effects that are being applied to a network. Note that this would be treated as truth data by the receiving application (i.e., it must not be visible to the players of the simulation (live, virtual or constructive) as its purpose is to allow applications participating in the simulation to apply the effects to their internal information passing network(s) or equipment). The data structure should include at least:
  - Activation status: Whether the effect is inactive or active;
  - Affected network: The network to which the effect is being applied, identified by its assigned ID; and
  - Parameters: The parameters of the attack, as applicable for the type of attack.

5.2 Technological Solutions

The implementation of the conceptual architecture would require technological solutions in a few distinct areas. These are:

- The ILEC implementation;
- The logical networks implementation;
- New or modified CGF application implementations;
- Behaviour implementation to react to information layer effects; and
- Data standards development and adoption.

This section reports on existing technologies, and proposes research and development activities.

5.2.1 Product-Based Solutions

5.2.1.1 Systems Tool Kit

Utility: ILEC implementation

Systems Tool Kit (STK) is a modelling environment commercialized by Analytical Graphics Inc. (AGI). STK has been used by ManTech International Corporation to model cyber effects in a degraded environment (ManTech, 2011).

STK is natively able to simulate specific effects, such as line of sight and range. Add-ons are available to extend the capabilities to cover other effects, in particular communications analysis and RF propagation effects or irregular terrain[7]. In ManTech's experiment (ManTech, 2011), the input to STK included:

- A scenario in time and space; and
- Physical system performance parameters such as platform and target positions and velocities, sensor performance parameters and communications systems parameters (including antenna size, system gain, transmit power, receiver sensitivity, frequencies, bandwidth and data transfer rates).

The physical and cyber effects output included:

- Collection time;
- Signal to noise ratio;
- RF propagation loss;
- Link budget;
- Latency;
- Bit error rate; and
- Data integrity/corruption.

It can be seen from this list that some information layer effects could be supported by STK, particularly the Environmental effects of interference, blockage and propagation loss. Using its API, it would likely be possible to extend the capabilities to include some of the Human effects

[7] A list of features along with the add-on that is necessary to cover them is available on AGI's website at http://downloads.agi.com/u/downloads/products/042114_FeatureComparison.pdf and at http://www.agi.com/downloads/products/product-literature/STK_ComponentsFlyer.pdf

from Table 4-2. Tools are also available to integrate STK in a distributed simulation environment.

STK may have some drawbacks that prevent it from being a viable solution. Experience with version 10 of STK[8] has confirmeda drawback in that STK does not have any artificial intelligence or built-in functions that allow it to adapt to the combat situation. In STK, scenarios are scripted along a timeline and the application will follow that script without responding to participant actions. Hence the tool is suitable for experimentation and systems analysis but not for training in a realistic environment where allies and enemies adapt to the situation. Additionally, experience with STK's performance suggests that high-end hardware may be required to run it for more intense scenarios. More research would be required to determine if some of the STK functions could be used inside an ILEC and/or a CGF implementation while circumventing other STK functions that have limited usefulness to the information layer effects implementation.

5.2.1.2 QualNet

Utility: The logical networks implementation

The QualNet communications simulation platform (QualNet), from Scalable Network Technologies, is a planning, testing and training tool that models the behavior of a real communications network. QualNet provides an environment for designing protocols, creating and animating network scenarios, and analyzing their performance. QualNet uses a standards-based implementation of protocol models. It can connect to other hardware and software applications.

In QualNet, a specific network topology is referred to as a scenario. A scenario allows the user to specify all the network components and conditions under which the network will operate. This includes: terrain details; channel propagation effects including path loss, fading, and shadowing; wired and wireless subnets; network devices such as switches, hubs and routers; the entire protocol stack of a variety of standard or user-configured network components; and applications running on the network.

QualNet integrates to varying degrees with product offerings from AGI, Presagis and MÄK Technologies.

5.2.1.3 EXata + Cyber

Utility: The logical networks implementation; ILEC implementation.

EXata is a network emulator tool from Scalable Network Technologies[9]. It uses a software virtual network to represent the network, the protocol layers, antennas and devices. The system

[8] MacNeil K. (2016), personal communication.
[9] Website: http://web.scalable-networks.com/content/exatacyber

can interoperate with real radios and devices, and real applications can run on the emulated network. EXata integrates with a Cyber Behaviour Model Library to implement cyber attacks.

Scalable Network Technologies used its products to develop a simulation of cyber threats to the entire Department of Defense net-centric infrastructure (project "StealthNet"[10]). This example demonstrates that EXata with the Cyber Library is a potential technological solution to simulate networks which support information layer effects. Hence it could be a candidate application for the logical networks implementation and for some of the ILEC functionality.

5.2.1.4 Network Defense Trainer

Utility: The logical networks implementation.

Network Defense Trainer (NDT) is another network emulator application from Scalable Networks Technologies[11]. It was released in the summer of 2014. Wihl (2015) is a white paper that provides a good overview of the product's capabilities and uses, including an example. The following account presents the major features and is reproduced from the Wihl (2015) paper:

> *In a cyberspace operation analysis, three factors - privacy, integrity and availability - are the measures of performance. A key challenge for training is to evaluate how these come to play in the larger context of mission effectiveness. For this reason, we chose to develop an architecture that could be integrated into live virtual constructive environments, so that the effects of compromised data privacy, integrity or availability would affect operational systems, humans in the loop, or constructive entities, resulting in changes in battlefield outcome. To achieve this, the system would need to integrate with Distributed Interactive Simulation (DIS) or High Level Architecture (HLA) based simulations while also being able to bring live battlefield application traffic and communications into and out of the emulated communications network. […]*
>
> *In classical domain training exercises, messages typically get passed directly between sender and receiver perfectly, without degradation. In cyber ranges, only host computers and networks are represented, without any kinetic battlespace representation. A new approach is to link these two disconnected training environments. Messages transmitted between entities in the classical domain are intercepted and sent through a software emulation of the battlefield network. As they traverse the emulated network, they are subjected to cyberspace operations which affect what gets delivered to the receiving entities. Messages that get through (which might have been delayed, eavesdropped or had selected information altered or dropped en route) are sent to the receiving entities in the classical domain. Compromised communications affect the entities' and trainees' situational awareness and decision-making, and therefore overall mission outcome.*

[10] http://web.scalable-networks.com/content/contract-development-projects
[11] Website: http://web.scalable-networks.com/content/network-defense-trainer-gov-and-mil-applications

The software emulation of the network, running in real-time, models the full network protocol stack on every emulated node and connects these nodes over simulated links that can be wired and wireless. Wireless communication effects include terrain, jamming, interference, fading, and other environmental factors. Actual packets are passed up and down the emulated protocol stack on every node and across the simulated physical layer between nodes. The emulated network thus reacts the same way as a real network, and can be subjected to real or simulated cyberspace operations.

A suite of simulated cyberspace attacks and defenses can interact with every layer of the emulated network. These include network security protocols, firewall models, port and network scanning, eavesdropping, jamming and silent jamming, denial of service, stimulation of intrusion detection systems, SIGINT, vulnerability exploitation, virus and worm propagation and defense, backdoors, rootkits, botnets, and others. Host models can be configured with memory, CPU cycles, vulnerabilities, processes, and shared files which can get infected. Security logs are generated to assist with forensics. Adaptive attack scripts can be used which will modify attack vectors depending on the success of previously attempted attacks.

The real-time software emulation of the network makes it possible to represent the communication infrastructure at sufficiently high levels of fidelity that live equipment, devices, and applications—such as sensor feeds, streaming video, and voice communications—can be deployed unmodified across it, and thus be subjected to cyberspace operations.

From this description, it appears that NDT is a capable application that solves some of the issues related to the implementation of information layer effects. For example, it includes a control interface that seems to implement the proposed ILEC control functions. However, it does not solve the issues related to the information exchange occurring internally to current CGF applications. The effects on HLA and DIS messages are also unclear as that aspect is not expanded upon in the paper. Finally, although NDT could help to implement training environments that bridge information warfare with *kinetic* battlespaces, it is a proprietary implementation. What is required is a standard-based approach that could be used without being locked into acquiring NDT.

5.2.1.5 NetSim

Utility: The logical networks implementation.

NetSim is a network simulator developed by Telcos[12]. NetSim allows the user to create networks using a GUI or Extensible Markup Language (XML) configuration files. The user can set properties for each network node and run the simulation while recording traces that report on parameters such as arrival time, queuing time, payload, overhead, and error causes. Analysis tools reveal metrics that include, among others, delay, loss and packet error.

[12] Website: http://www.tetcos.com/netsim_gen.html

NetSim has been developed to model the five-layer TCP/IP stack. It allows the use of a variety of protocol standards. Wireless propagation is implemented in NetSim. Development of cyber-attacks and environmental effects is possible by custom coding them to the desired level of fidelity directly into the published NetSim protocol source code. The Telcos website includes a video that shows how to create a "sinkhole", in this case being used as a spoofing example. Network sinkholes can also be used to defend against attacks.

5.2.1.6 CGF Products

There are several CGF solutions available from both private companies and government institutions. Marquette (2013) provides a list of these with a summary of capabilities. This section provides information on a few CGF products with a focus on how information sharing is modelled.

NOTE: Requests for information were sent to various CGF vendors. The information provided in this section reflects the answers that were received. For cases where limited or no information was received, it is possible that the products are able to do more than is described in this section.

5.2.1.6.1 MÄK Technologies VR-Forces

Utility: new or modified CGF implementations.

VR-Forces is MÄK Technologies' CGF application. It integrates with other MÄK products to extend its capabilities, including the B-HAVE product which provides artificial intelligence behaviour modelling.

In its current implementation (version 4.3), messages between VR-Forces entities are disseminated to all entities of the same force, regardless of distance or terrain blockage. There are plans for this implementation to change in a future version of VR-Forces. Input from MÄK Technologies[13] provided insight on the planned changes. These plans are preliminary and are subject to change, but are nevertheless in the works. In essence, MÄK plans on implementing a simple network model in VR-Forces. Entities would be able to connect to networks and exchange information on them. The format of the information is not going to be modelled (i.e., it will remain the same as the messages that are currently being sent between entities in VR-Forces instead of following a standard such as C-BML). At this time MÄK does not envision messages being allowed to flow from one network to another.

Plugins for MÄK's network implementation could be written to support an information layer implementation. The plugins could be used to extend the basic functionality that will be offered, for example to customize the messages, to interface with external applications or to manage the parameters of specific network types.

[13] Dillman B. (2016), personal communication.

Hence, it is probable that a significant effort would be required to make VR-Forces comply with the conceptual architecture presented in paragraph 4.3. MÄK has mentioned that they would welcome any input on these plans, so it may be beneficial to keep them abreast of any progress that would be made in the adoption of a conceptual architecture for an information layer. Other vendors would likely benefit as well.

5.2.1.6.2 Bohemia Interactive VBS3

Utility: new or modified CGF implementations.

VBS3 is a simulation training solution which includes several components, including among others a CGF component and a radio simulator. It is widely used by several armed forces across the world, including the Canadian Armed Forces.

VBS3 comes with product named *VBSRadio*. It enables radio and direct voice communications between participants. The Pro version features distance-based degradation that can also be influenced by weather effects within the simulation.

5.2.1.6.3 MASA Sword

Utility: new or modified CGF implementations.

SWORD is a constructive simulation developed by MASA in France. Although it simulates individual entities, its main utilisation is to train commanders in maintaining situational awareness and issuing orders. Platoons and companies are autonomous, and the developer mentions that these forces can adapt to changes in situation and environment. Doctrines can be customized.

SWORD manages information exchange between groups of entities via “knowledge groups”. A knowledge group is composed of one or more entity groupings and their subordinate entities. Each member of a knowledge group shares its situational awareness knowledge with the other members instantaneously and completely, except under specific circumstances. The overall knowledge of the group is maintained in a knowledge database. However, each entity grouping and also each individual entity has its own knowledge database, and they are synchronized with the knowledge group’s database except in the following cases:

- Each knowledge group has a leader. If an entity or entity grouping is out of range of the leader or blocked by terrain features, then the out-of-range entity(ies) stop sending updates to and receiving updates from the knowledge group, causing their own database(s) to be unsynchronized with the knowledge group’s.

- When an entity’s communications are being jammed or the entity is in total radio silence, then the entity stops sending and receiving updates from others, causing its knowledge database to be unsynchronized.

- When an entity is in radio silence for transmissions only, it still receives updates from its parent group but does not send updates to it. Hence, its knowledge base has the full situational awareness information (less the information from other entities that are also in radio silence), but its parent group does not have the information generated by the entity.

- When an entity is in radio silence for reception only, the entity sends updates to its parent group but it does not receive updates from the parent group. Hence the parent group has the full situational awareness information, but the entity does not.

Two knowledge groups will exchange situational awareness information when their respective leaders are in range from one another. In that case, their knowledge databases get synchronized. However there can be a hierarchy in the knowledge groups, i.e., a knowledge group can be subordinate to another. In that case, updates received from another knowledge group by a superior will not be shared instantaneously with subordinate knowledge groups. Instead, it will be sent down on a periodic basis whose period is configurable.

Entities in SWORD act depending on the situational awareness information that they have in their own knowledge database. Hence if their information is not up-to-date, they may take actions that are contrary to what they would be doing if they had updated information. Their behaviour also depends on several factors, including the rules of engagement, the mission, the firepower ratio compared to the enemy's, and the entity's evaluation of the geostrategic context.

SWORD offers an API through which an external application could access the knowledge group information and each knowledge group's knowledge database. It is also possible for an external application to add or remove information from the database.

All communications between entities in SWORD are currently implemented as radio communications. MASA is looking into the possibility of adding other communication mechanisms as part of the research and development projects, however no timeline has been provided.

5.2.1.6.4 Presagis STAGE

Utility: new or modified CGF implementations.

STAGE from Presagis is a simulation development environment that can integrate with other Presagis and third-party tools to support simulations and experiments. It offers AI capabilities using AI.Implant, helping to generate more realistic entity behaviour, primarily focused on entity movement.

STAGE integrates with QualNet to enable realistic communication effects. The partnership between Presagis and Scalable Network Technologies was announced in 2010 and aimed at "adding the rigors and uncertainties of in-field communications like urban environment effects,

message delays or drops, signal jamming and sophisticated cyber attacks"[14]. QualNet is no longer being offered through Presagis. It may still be possible to connect STAGE with QualNet through a STAGE plugin.

5.2.1.6.5 OneSAF

Utility: new or modified CGF implementations.

OneSAF is an entity-level simulation that supports both CGFs and semi-automated forces applications.

Brown J.C. (2009) reported on the research and development efforts that were ongoing at the time for the integration of electronic warfare functions in OneSAF. Parts of the presentation confirm that OneSAF includes extensive RF propagation models and also ground-based and air-based jamming. Urban area RF propagation calculations are done in real time in OneSAF. OneSAF has also been integrated with EXata to model several types of networks, and threat agents were incorporated to attack the networks across land, surface, air and space with physical, electromagnetic and cyber-attacks. Additionally, a proof-of-concept demonstration simulated cyber-attacks on the port of San Diego, disrupting radio communications, hacking the automated identification system and running denial of service attacks on servers. Hence it appears that OneSAF has already demonstrated the capability of incorporating a subset of the information layer effects that have been identified in Table 4-2.

5.2.2 Agent-Based Solutions

5.2.2.1 DARNOS

Utility: Behaviour implementation to react to information layer effects; ILEC implementation.

DARNOS is an agent-based modelling and simulation tool that uses an organization-oriented approach to model the dynamic interactions among the entities of a networked force. The dynamic interactions include information exchange, decision-making and action. The developers emphasized the dynamic management and representation of the information environment. Hence, the DARNOS project fell along the lines of what would be required to implement an information layer and possibly also information layer effects. Unfortunately at this time it appears that the project is at a stand-still or has been abandoned. No papers have been published on DARNOS since 2008.

The architecture of DARNOS influenced the conceptual entity architecture suggested in paragraph 4.3.2.3. The DARNOS approach is certainly worth exploring for the implementation of an information layer.

[14] See announcement at http://www.presagis.com/about_us/press_room/releases/presagis_partners_with_scalable_network_technologies_to_bring_high_fidelity_communications_modeling_to_stage/

5.2.2.2 CAST

Utility: Behaviour implementation to react to information layer effects; new or modified CGF implementations.

One approach that could be useful for an information layer implementation and its effects is to use a multi-agent architecture to model teamwork. The Collaborative Agents for Simulating Teamwork (CAST) architecture was designed in the early 2000s at the Texas A&M University. Malhotra (2009) summarizes the goals and capabilities of the CAST, while Yen (2001) details its architecture. CAST enables a team of agents to establish a shared mental model by anticipating other agents' information needs and proactively choosing whether to inform others about information. The architecture also incorporates information fusion capabilities.

Most papers that CAE found about CAST date from the first half of the 2000 decade. It is not clear if more work is currently being performed on this architecture. On the surface, it looks like an architecture that could be useful for implementing information layer concepts, as one of the most important aspects of the CAST architecture is its focus on proactive information sharing.

5.2.2.3 JACK and Derivatives

Utility: Behaviour implementation to react to information layer effects; new or modified CGF implementations.

JACK applications consist of a collection of autonomous agents that take input from the environment and communicate with other agents[15]. The agents use the BDI foundation to manage the behaviour of the entities and the complexity of the problem space.

CoJACK is a BDI cognitive architecture that can use degrading factors such as fatigue and fear to influence the behaviour of agents. It has been successfully integrated with VBS2 (Evertsz, 2009) to increase the realism of the behaviour of entities in a suicide bomber scenario.

JACKTeams supports the definition of autonomous teams of agents, representing the social relationships and coordination between team members.

All of the JACK line of products is developed by Agent Oriented Software (AOS) in collaboration with several partners. These products have been used in many research applications and are amongst the most mature multi-agent applications, having been active for close to 20 years. This line of products should be explored when considering agent technologies to implement the cognitive layer of the entity conceptual architecture. With its ability to model team behaviour, it could also be used for the organizational structure representation in CGFs.

5.2.2.4 MASA Life

Utility: Behaviour implementation to react to information layer effects.

[15] Website: http://aosgrp.com/products/jack/

MASA Life[16] is an agent-based middleware that enables the creation of autonomous behaviours in simulations. It offers a visual building block, tree-based interface to design agent behaviours. Plugins for several existing products, including VBS2, are available.

For an information layer implementation, MASA Life could be used to control the behaviour of entities in response to changes in the received information. It may be possible to use this product for the cognitive layer of the entity architecture. The ability of a MASA Life-based entity to control other entities in a team context is demonstrated in a video available on the website, however it is not mentioned whether or not the entities can share information and perform data fusion.

5.2.3 Data Structure Solutions

5.2.3.1 Coalition Battle Management Language

Utility: Behaviour implementation to react to information layer effects; data standards development and adoption.

The Coalition Battle Management Language (C-BML) is a standard that is currently being developed under the direction of SISO. Blais (2011) provides a very good overview of the standard. The standard is being developed in three phases and is currently in phase 2, with phase 1 having been approved in April 2014.

C-BML can be used as a message payload to express information included in plans, orders, requests and reports. Phase 1 saw the development of message constructs. Phase 2 is developing a formalized grammar (syntax, semantics, and vocabulary). Phase 3 will involve specification of a battle management ontology.

C-BML offers the potential to define how information moving around the information layer can be constructed so that it can be recognized by any C-BML compliant system, real or simulated. With respect to information layer effects, some of the Phase 1 constructs could potentially be used to order information operations/warfare actions or report on the occurrence of information operations/warfare actions. Excerpts from the “OtherActionEvent/CategoryCode” elements of the “cbml-action-types” schema are provided at Appendix B as examples of events that relate to information warfare effects. How these elements could be used in messages will be defined in Phases 2 and 3 of the development of the C-BML standard.

With the expectation that this standard will eventually be adopted and offer improved interoperability between systems from multiple provenance, the use of C-BML should be explored as part of an effort to define the information layer and information layer effects. This could include proposing additional elements to the C-BML Standard authority for inclusion in future amendments to the standard, so as to help define ways to order or report cyber-attacks in particular.

[16] Website: http://masa-group.biz/products/life/

5.2.3.2 Military Scenario Definition Language

Utility: Data standards development and adoption.

MSDL is a SISO standard that was first published in 2008 and re-affirmed in 2015. The standard is still in evolution and there are plans to eventually align it with the C-BML standard so that they can seamlessly interoperate. MSDL is an XML schema-based implementation of standardized scenario constructs that can be used and re-used to define the initialization state or snapshot state of a scenario.

Some of the constructs in MSDL describe the truth data while other constructs describe the *intelligence* information that each force has about other objects in the scenario. However it does not include provisions for assigning tasks and plans to entities. This is one of the goals that the SISO working groups are aiming in their effort to align MSDL with C-BML, i.e., to be able to assign plans, orders and tasks using the C-BML format.

With respect to the implementation of an information layer, MSDL can help to define initial information in a scenario, especially using its intelligence constructs. When it is aligned with C-BML, it will allow sharing information about plans, orders and tasks. It does not include any provisions at present to define which communication networks exist; that will have to be considered during the development of the data constructs required to implement the conceptual architecture proposed in paragraph 4.3.

NOTE: A communication received in March 2016 indicates that the NATO Modelling and Simulation Group (NMSG) has commenced work on merging the C-BML and MSDL standards into a single standard named C2SIM. The kick-off meeting on MSG-145, *Operationalization of Standardized C2 Simulation Interoperability*, took place from 9 to 11 March 2016.

5.2.3.3 C2 BOM

Utility: Data standards development and adoption; logical networks implementation.

Dillman (2009) proposed a BOM for networked C2 information. This C2 BOM aims to provide a generalized model of exchanging C2 operational picture information between not only entities, as is usually the case in HLA Federations, but between systems or components on one or more interconnected networks. The C2 BOM is compatible with DIS-compliant simulations.

The C2 BOM incorporates a conceptual model for the C2 networks and a conceptual model for the C2 data. The C2 network model uses a publish-and-subscribe model, without specifying the protocol used to exchange data. It does not incorporate authentication and authorization constructs. To summarize the model, a logical network has zero or more nodes that have zero or more published and/or subscribed objects produced by zero or more publishers and subscribers. A network node can be connected or disconnected from a logical network. Published objects have attributes for creation time, last change time and expiry time.

The data model incorporates five layers which define different phases in the development of a common operational picture. Level 1 is unmodified raw data. Level 2 is the first level of processed data, providing interesting measurements based on the raw data. Level 3 processes level 2 data further to generate correlated data from one or more sensors from a single platform. Level 4 represents a state estimate for a platform based upon a correlated set of level 3 items. Level 5 is the most complete estimate of a single entity based upon all information available for that entity.

The C2 BOM network and data models could be used as a foundation to start developing the data structure for an information layer. The network model could form the basis of the logical networks description that must be exchanged between the participants of a simulation, but it must be extended to deal with issues such as encryption, authorization and authentication. The data model could be used to help develop how participants could build and exchange situational awareness information across the networks.

5.3 CGF Compatibility with Proposed Architecture

More information is required from vendors to determine the compatibility of existing CGFs with the proposed architecture. On the surface, it appears that some of the components of the architecture could already be supported to some level. For example, the integration of STAGE with QualNet suggests that the representation of the networks present in a simulation is already possible. Also, various studies in the past have developed agents that could cover some of the requirements of the cognitive layer in the entity conceptual model. Other projects have worked towards improving C2 structures and information passing.

In general, existing CGFs provide an API that allows developers to build plug-ins that incorporate functionality that is not present in the out-of-the-box version of the CGF. It may be possible to use those APIs to incorporate some of the concepts suggested by the conceptual architecture. A previous project that CAE participated in provides a case in point: CAE modified a component attached to VR-Forces entities so that combat engagements between two entities would be handled by an engagement server instead of by the built-in engagement algorithms of VR-Forces. In the same way that the handling of engagements was rerouted, it may be possible to reroute message handling so that the messages are handled by an ILEC instead of the CGF's normal processing. In other cases, plugins may be written to extend existing functionality to customize it to fit the needs of an information layer.

5.4 A Short-Term Partial Solution – MOM Method

In an HLA federation, federates subscribe to and publish objects and interactions. The objects and interactions contain information as defined in the FOM (or collection of FOM modules in the case of HLA-Evolved). When an entity sends information to another entity that is in a different federate, for example a simulator that has joined the federation, then an ILEC may be constructed in such a way that it will see the information transfer and may impose an information layer effect on it. The limitation is when the other entity is within the same federate, such as a CGF. Depending on the CGF implementation, the information transfer may not

necessarily be made through HLA. Rather, it may be done entirely within the CGF executable. In that case, the ILEC will have no visibility into the information transfer and will be unable to affect it.

Rogers (2000) describes a method whereby the HLA MOM services are used to intercept and manage the communications between federates. The main advantage of this approach is that it is transparent to other federates and thus, it should function with pre-existing federates. On the other hand, there are at least three important disadvantages to the approach. First, as mentioned above, it works only for communications between federates, meaning that it does not affect communications taking place between entities that are managed and controlled entirely within an application as would be the case for a CGF. Second, any effect applied against a federate would apply to every object controlled by that federate. For example, if the affected federate is a CGF and the intent is to calculate and apply range-based delays to the communications emanating from a specific CGF entity, all entities managed by the CGF will be affected by the delay. Third, the method increases network traffic, possibly going as far as doubling it. Hence the method may be unusable for larger distributed simulations. Although these disadvantages present compelling reasons to consider other approaches, it remains that this method's main advantage could make it a good choice for an interim solution, until a better approach is developed.

An example of the use of HLA MOM services for a jamming scenario in which a specific federate is targeted (for example a simulator) is as follows:

1. The ILEC invokes the *RequestPublications*, *RequestSubscriptions* and *RequestOwnedObjects* HLA MOM services. These actions allow the information layer federate to build a list of the objects and interactions that are published by, subscribed to and owned by each federate.

2. Using the ILEC GUI, an instructor specifies which federate is targeted and specifies which mediums are to be jammed.

3. The ILEC determines which information being published over the medium is subscribed to by the targeted federate. Then:

    a. The ILEC keeps a record of these subscriptions.

    b. The ILEC uses the *UnsubscribeInteractionClass* HLA MOM service on behalf of the targeted federate to stop information flowing to that federate over the specified medium.

    c. When the instructor indicates through the GUI to stop the jamming action, the ILEC uses the SubscribeInteractionClass HLA MOM service to re-establish the flow of information, using the recorded data.

4. The ILEC determines which information the target federate publishes over the medium. Then:

   a. The ILEC keeps a record of these publication parameters.

   b. The ILEC uses the *UnpublishInteractionClass* HLA MOM service on behalf of the targeted federate to stop information flowing from that federate over the specified medium.

   c. When the instructor indicates through the GUI to stop the jamming action, the ILEC uses the PublishInteractionClass HLA MOM service to re-establish the flow of information, using the recorded data. This would be done simultaneously to the re-establishment of the interactions subscriptions.

6 CONCLUSIONS AND FUTURE WORK

6.1 Conclusions

This report detailed the results of a literature review on the state of information layer research and development, and proposed a conceptual architecture to implement an information layer and information layer effects. It also included a survey of various technologies that could be useful for the implementation of the conceptual architecture. The following conclusions apply:

1. Relatively little research has been carried out to devise ways to implement information layer effects in battlefield simulations. Most of the research and development regarding information layer effects in simulations has been oriented towards simulation systems to train network administrators and technicians or to test defensive systems.

2. With very few exceptions, existing CGFs do not support the concept that information exchange between force elements is carried out over several computer and non-computer networks and using a variety of communication methods, each of which is susceptible to information warfare attacks.

3. The concept of information layer includes not only the movement of information, but also the generation of information to include the application of biases and data interpretation.

4. Several research projects have been conducted over the last 15 years to develop artificial intelligence agents that can react to changes in the battlefield situation. These agent-based solutions could be applied to react to information layer effects. Reaction examples include taking detrimental actions caused by disinformation, finding alternate means of communications when an information warfare attack is discovered, assessing the reliability of information, and so on.

5. Some research carried out in the first half of the 2000s decade showed promise, but no recent articles were found that could ascertain the status of these efforts. This is the case in particular for the DARNOS project, for MANA-related work and for WISDOM-II development.

6. Very few published research papers report on efforts to develop data structures that support the implementation of information layer effects in distributed simulations.

7. A conceptual architecture for the implementation of an information layer and its effects is presented in Section 4. The proposed architecture supports the implementation of all information layer effects described in paragraph 4.2.3 of the report.

8. The conceptual architecture is presented using four different views, each of which concentrates on a different aspect of the architecture. The architecture can be applied to a single CGF application or to a collection of components, with the application of information layer effects being loosely coupled from other components.

9. The conceptual architecture supports concepts such as dynamic organizational structures, command and control relationships, and data fusion.

10. The conceptual architecture requires that communication network structures be known and shared amongst the applications participating in a simulation. Current data structures and distributed simulation protocols do not support this requirement. Hence, research and development effort needs to be expended to develop support for this requirement.

11. When implementing the conceptual architecture, the ILEC could be a stand-alone application that monitors and affect information exchange traffic, or it could be an application that attaches to one or more participating applications. Both approaches have their advantages and disadvantages.

12. Several existing technologies could be used to help implement the conceptual architecture. No single application meets all the requirements of the architecture. Scalable Network Technologies' Network Defense Trainer seems to have the most commonality with the architecture. MASA Group's SWORD seems to be the CGF that addresses the most information layer requirements, although much work remains to be done to yield a complete solution.

13. C-BML should be explored as part of an effort to define the information layer and information layer effects. It already incorporates some data structures that could be useful but does not currently directly address the data requirements for the information layer and its effects.

14. Expansion to MSDL should be considered when defining the data structures to support the information layer and its effects. In particular, the requirement to define which communication networks exist in a simulation would be an important scenario parameter to include in an MSDL description of a scenario.

15. Efforts to merge MSDL with C-BML have commenced. This effort may yield a new standard.

16. The C2 BOM network and data models could be used as a foundation to start developing the data structure for an information layer.

17. Existing CGFs are not fully compatible with the proposed conceptual architecture. Some aspects of the architecture could be incorporated using a CGF API when one exists.

6.2 Suggestions for Future Work

The implementation of an information layer and its effects will require research and development. The following suggestions for future work could be a starting point:

1. There is a need to develop a standardized method to share networks structure information between applications participating in simulations. Additionally, data structures that support the description of information layer effects need to be developed and standardized.

2. There is a need for agents that can assess the timing, relevance and validity of data being received, and to fuse the data with other sources. There is a need to leverage the work that is already being done on this subject.

3. There is a need to develop an entity structure that can react to information layer effects in a way that is representative of real world reactions/adaptation to similar effects. This structure would likely be implemented using agents.

4. There is a need to model and implement information layer effects in CGFs and in distributed simulations. Very few CGFs currently support information layer effects, and the distributed simulation protocols have no or very little explicit support for these effects.

APPENDIX A ADDITIONAL INFORMATION

A.1 Acronyms

Acronym	Definition
AAR	After Action Review
AGI	Analytical Graphics Inc.
AI	Artificial Intelligence
AOS	Agent-Oriented Software
API	Application Programming Interface
BDI	Belief-Desire-Intention
BOM	Base Object Model
C2	Command and Control
C2SIM	Command and Control Simulation
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAAJED	Cyber And Air Joint Effects Demonstration
CAS	Close Air Support
CAST	Collaborative Agents for Simulating Teamwork
C-BML	Coalition Battle Modelling Language
CEDA	Capability Engineering Design Approach
CGF	Computer-Generated Forces
CIA	Confidentiality, Integrity and Availability
DAF	Defence Architecture Framework
DARNOS	Dynamic Agents Representation of Networks of Systems
DIS	Distributed Interactive Simulation
DSTO	Defence Science and Technology Organisation

Acronym	Definition
EW	Electronic Warfare
FLEW	Force Level Electronic Warfare
FOM	Federation Object Model
GUI	Graphical User Interface
HLA	High Level Architecture
IAS	Internet Attack Simulator
ILEC	Interface Layer Effects Controller
IO	Information Operations
ITI	Information Technology Infrastructure
LVC	Live, Virtual and Constructive
MANA	Map Aware Non-Uniform Automata
MOM	Management Object Model
M&S	Modelling and Simulation
MSDL	Military Scenario Definition Language
NCW	Network Centric Warfare
NDT	Network Defense Trainer
NMSG	NATO Modelling and Simulation Group
RF	Radio Frequency
SA	Situational Awareness
SISO	Simulation Interoperability Standards Organization
STK	Systems Tool Kit
STORM	Socio-cultural Teamworking for Operational Research Models
TA	Technical Authority
UAV	Unmanned Air Vehicle
UK	United Kingdom

Acronym	Definition
VCCI	Virtual Command and Control Interface
WISDOM	Warfare Intelligent System for Dynamic Optimization of Missions
XML	Extensible Markup Language

APPENDIX B EXCERPTS FROM C-BML STANDARD

The following excerpts from the “OtherActionEvent/CategoryCode” elements of the “cbml-action-types” schema are examples of action events that could be reported and that could relate to information warfare effects:

Kind	Value	Annotation
enumeration	ATTEL	**Documentation:** <Definition xml:lang="en">Conducting electronic warfare involving the use of electromagnetic energy, directed energy or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.</Definition> **appinfo:** <DisplayValue xml:lang="en">Attack, electronic</DisplayValue>
enumeration	BREACH	**Documentation:** <Definition xml:lang="en">Breaking through or securing a passage through an enemy defence, obstacle, minefield, or fortification.</Definition> **appinfo:** <DisplayValue xml:lang="en">Breaching</DisplayValue>
enumeration	CLRRAD	**Documentation:** <Definition xml:lang="en">Eliminating transmissions on a tactical radio net in order to allow a higher precedence transmission to occur.</Definition> **appinfo:** <DisplayValue xml:lang="en">Clearing, radio net</DisplayValue>
enumeration	COMACT	**Documentation:** <Definition xml:lang="en">The enabling of transmission of information.</Definition> **appinfo:** <DisplayValue xml:lang="en">Communications activation</DisplayValue>
enumeration	COMDEA	**Documentation:** <Definition xml:lang="en">The disabling of transmission of information.</Definition> **appinfo:** <DisplayValue xml:lang="en">Communications deactivation</DisplayValue>
enumeration	COMDIS	**Documentation:** <Definition xml:lang="en">Interruption of the passage of communications by natural or man-made phenomena.</Definition> **appinfo:** <DisplayValue xml:lang="en">Communications disruption</DisplayValue>

Kind	Value	Annotation
enumeration	COMINT	**Documentation:** <Definition xml:lang="en">Capturing electromagnetic communications signals.</Definition> **appinfo:** <DisplayValue xml:lang="en">Communications interception</DisplayValue>
enumeration	COMRES	**Documentation:** <Definition xml:lang="en">The reestablishment of the ability to communicate.</Definition> **appinfo:** <DisplayValue xml:lang="en">Communications restoration</DisplayValue>
enumeration	DCPTEL	**Documentation:** <Definition xml:lang="en">In electronic countermeasures, the deliberate radiation, re-radiation, alteration, absorption or reflection of electromagnetic energy in a manner intended to confuse, distract or seduce an enemy or his electronic systems.</Definition> **appinfo:** <DisplayValue xml:lang="en">Deception, electronic</DisplayValue>
enumeration	DCPTIN	**Documentation:** <Definition xml:lang="en">Employing measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests.</Definition> **appinfo:** <DisplayValue xml:lang="en">Deception</DisplayValue>
enumeration	DENYNG	**Documentation:** <Definition xml:lang="en">Preventing access by blocking, disrupting, dislocating and/or bringing fire to bear.</Definition> **appinfo:** <DisplayValue xml:lang="en">Denying</DisplayValue>
enumeration	ELCWAR	**Documentation:** <Definition xml:lang="en">Military action to exploit the electro-magnetic spectrum encompassing the search for, interception and identification of electro-magnetic emissions, the employment of electro-magnetic energy, including directed energy, to reduce or prevent hostile use of the electro-magnetic spectrum, and actions to ensure its effective use by friendly forces.</Definition> **appinfo:** <DisplayValue xml:lang="en">Electronic warfare</DisplayValue>
enumeration	INDESP	**Documentation:** <Definition xml:lang="en">The practice of spying or the use of spies to obtain information about the plans and activities of competitors.</Definition> **appinfo:**

Kind	Value	Annotation
		<DisplayValue xml:lang="en">Industrial espionage incident</DisplayValue>
enumeration	INTCPN	**Documentation:** <Definition xml:lang="en">Conducting electronic warfare support operations with a view to searching, locating and recording radiated electromagnetic energy.</Definition> **appinfo:** <DisplayValue xml:lang="en">Interception</DisplayValue>
enumeration	ISSMDA	**Documentation:** <Definition xml:lang="en">Sending forth or putting into circulation a non-fictional essay, especially one included with others in a newspaper, magazine, or journal.</Definition> **appinfo:** <DisplayValue xml:lang="en">Issuing media article</DisplayValue>
enumeration	ISSMDD	**Documentation:** <Definition xml:lang="en">Sending forth or putting into circulation any document published on a media that provides a factual record or report.</Definition> **appinfo:** <DisplayValue xml:lang="en">Issuing media documentary</DisplayValue>
enumeration	ISSPRS	**Documentation:** <Definition xml:lang="en">Sending forth or putting into circulation an official statement issued to media for information.</Definition> **appinfo:** <DisplayValue xml:lang="en">Issuing press release</DisplayValue>
enumeration	JAMMNG	**Documentation:** <Definition xml:lang="en">Deliberately radiating, re-radiating or reflecting electromagnetic energy with the object of impairing the use of electronic devices, equipment or systems being used by the enemy.</Definition> **appinfo:** <DisplayValue xml:lang="en">Jamming</DisplayValue>
enumeration	NETSEI	**Documentation:** <Definition xml:lang="en">Taking electronic control of a communications network.</Definition> **appinfo:** <DisplayValue xml:lang="en">Network seizure</DisplayValue>
enumeration	PENTRT	**Documentation:** <Definition xml:lang="en">Breaking through the enemy's defence or disrupting the enemy's defensive systems.</Definition> **appinfo:** <DisplayValue xml:lang="en">Penetrating</DisplayValue>

Kind	Value	Annotation
enumeration	PROTEL	**Documentation:** <Definition xml:lang="en">That division of electronic warfare involving actions taken to ensure effective friendly use of the electromagnetic spectrum despite the enemy's use of electromagnetic energy.</Definition> **appinfo:** <DisplayValue xml:lang="en">Protection, electronic</DisplayValue>
enumeration	PSYOP	**Documentation:** <Definition xml:lang="en">Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behaviour of foreign governments, organisations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behaviour favourable to the originator's objectives.</Definition> **appinfo:** <DisplayValue xml:lang="en">Psychological operation</DisplayValue>
enumeration	PUBMDA	**Documentation:** <Definition xml:lang="en">Making generally known a non-fictional essay, especially one included with others in a newspaper, magazine, journal, etc.</Definition> **appinfo:** <DisplayValue xml:lang="en">Publishing media article</DisplayValue>
enumeration	PUBMDD	**Documentation:** <Definition xml:lang="en">Making generally known any document published on a media that provides a factual record or report.</Definition> **appinfo:** <DisplayValue xml:lang="en">Publishing media documentary</DisplayValue>
enumeration	PUBPRS	**Documentation:** <Definition xml:lang="en">Making generally known an official statement issued to media for information.</Definition> **appinfo:** <DisplayValue xml:lang="en">Publishing press release</DisplayValue>
enumeration	REORGN	**Documentation:** <Definition xml:lang="en">Changing a task organisation for a particular operation. (Normally takes place before an operation). This includes the transfer of authority.</Definition> **appinfo:** <DisplayValue xml:lang="en">Reorganising</DisplayValue>
enumeration	SABOTG	**Documentation:** <Definition xml:lang="en">An act or acts with intent to injure, interfere with, or obstruct the national defence of a country by wilfully injuring or destroying, or attempting to injure or destroy, any national defence or war

Kind	Value	Annotation
		material, premises or utilities, to include human and natural resources.</Definition> **appinfo:** <DisplayValue xml:lang="en">Sabotage</DisplayValue>
enumeration	SECCMP	**Documentation:** <Definition xml:lang="en">A release of information to someone unauthorised.</Definition> **appinfo:** <DisplayValue xml:lang="en">Security compromise</DisplayValue>
enumeration	SECVIO	**Documentation:** <Definition xml:lang="en">An infringement of a security protocol.</Definition> **appinfo:** <DisplayValue xml:lang="en">Security violation</DisplayValue>
enumeration	VERFYN	**Documentation:** <Definition xml:lang="en">Testifying to, asserting, affirming or confirming, as true or certain.</Definition> **appinfo:** <DisplayValue xml:lang="en">Verifying</DisplayValue>