Use Case Analysis of the Information Warfare Engagement Model Architecture

Mark G. Hazen
DRDC Atlantic Research Centre
9 Grove St, Dartmouth, NS
CANADA

Mark.hazen@drdc-rddc.gc.ca

Evan Harris & Tab Lamoureux
CAE Inc.
350 Legget Dr,
Ottawa, ON, K2K 2W7
CANADA

evan.harris@cae.com / tab.lamoureux@cae.com

ABSTRACT

The military battlespace is often visualized as set of layers representing different aspects, ranging from physical terrain to information flows. Computer Generated Forces simulations used for campaign and mission simulation have traditionally focused on the physical representation of units, terrain and effects.

In 2016, a layered simulation architecture was proposed to guide the evolution of Computer Generated Forces to include Information Warfare effects. Using a use-case of supporting the collective training of naval staff officers in information warfare, the simulation architecture description was further developed. Detailed descriptions of layer functionality and content were developed, along with inter- and intra-layer data flows. From these descriptions an initial data model was developed to facilitate an analysis of the utility of current interoperability data models for this application. This work lays a foundation for the specification of a common architecture for the simulation components required to model information warfare effects. It is hoped that such an architecture will facilitate the building of information warfare engagement models, the specification of interoperability standards, and the development of interoperable components.

1.0 INTRODUCTION

Traditionally computer generated forces (CGF) and semi-automated forces (SAF) simulations have concentrated upon force-on-force behavior and kinetic engagements. Often, command and control (C2) is implemented by simple condition reaction rules or direct human subject matter expert (SME) intervention. Further, in many instances inter-unit communication links have perfect fidelity and full information content. In an era of increased amounts and access to information, warfare has also evolved to take advantage of those systems, and deny them to the adversary. This information warfare (IW) includes both traditional and evolving network/cyber technologies, and CGF must also evolve in order to represent the effects of IW on the battlefield. It is worth noting that these IW operations are often aimed at changing the behaviour of decision-makers, not at changes in the physical environment, and thus it is the secondary and tertiary, or cumulative effects, that are finally seen in the physical layer as changed behaviour of adversaries or non-combatants.

In previous work [1] the authors advanced the argument that the use of a common architecture to guide the evolution of CGF should provide benefits in the future to enterprise implementations, while giving developers and industry the freedom to use innovative techniques to address the complex questions of IW. A conceptual IW simulation architecture was developed and it was recommended that a top-down, use-case based investigation of layer functionality and required data model should be undertaken as the next step in the development. MSG-ET-044 [2] has also recommended the development of common architecture elements at the game engine level of simulation.

Following initial work by Kearse [3] using a high-level use-case analysis that validated this general approach, Canada initiated a work program to conduct a more detailed use-case analysis. Initial results, aimed at mission-level cyber warfare, were contributed to NMSG 151 [4]. This paper provides an overview of the use-case analysis process and the main results, incorporating feedback from the NMSG 151 workshop, from applying the process to a naval training use-case. Additional details and the full results of the analysis will be available in the task report [5].

The aim of this paper is twofold, firstly to report on advances in the development and validation of a common simulation architecture for extending warfare modelling to include IW, and secondly to provide a launching point for others to extend the analysis with other use-cases.

INFORMATION WARFARE ENGAGEMENT MODEL ARCHITECTURE

Figure 1 shows the starting architecture for the current work, as presented at NMSG 143 in October 2016. In this IW conceptual model, the central nature of the communications layer is represented via the addition of information flows. It also acknowledges the separation of internal entity knowledge and external information sources. It assumes that entities only communicate via the communications layer and that all knowledge of the physical layer is generated by sensors via reports transmitted through a communications network (even for internal entity sensors).

In the architecture, IW activities are ordered/initiated from the cognitive layer and implemented by units in the physical layer, but the IW activities themselves take effect in either the communications layer (jamming, denial of service etc.) or within the elements of the information layer (changes to data, filtering of reports with respect to biases etc.). The ultimate effect of the operations is to change the adversary’s activities in the cognitive layer, with observable effects in the behaviour of units in the physical layer.

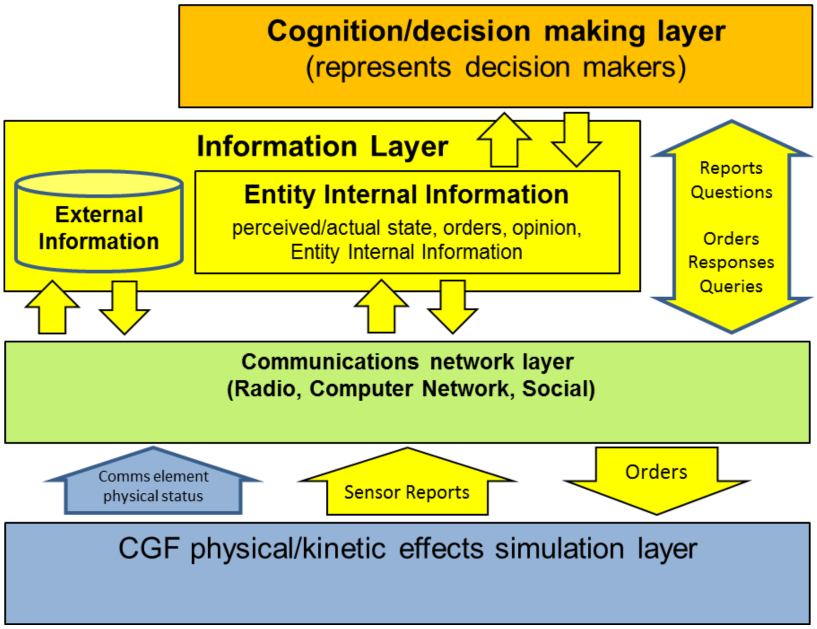
Cognition/decision making layer
(represents decision makers)
Information Layer
External Information
Entity Internal Information
perceived/actual state, orders, opinion, Entity Internal Information
Reports
Questions
Orders
Responses
Queries
Communications network layer
(Radio, Computer Network, Social)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

Figure 1: Information Warfare engagement model architecture, Version 1 (2016). [1]

One of the aims of the IW architecture is to provide a framework to develop and federate services representing differing fidelities of IW effects to match the requirements of different IW use cases. Thus, the architecture encourages the evolution of CGF away from highly integrated internal components towards a service based functionality that would be amenable to federation with third party or external modules. This encourages multiple implementations of each service, allowing different fidelity levels and security classifications, but also increases the complexity of the architecture. Thus, for example, changing the commander of a unit might involve switching from a cognitive layer service representing one type of commander (aggressive) to another (cautious). This modular approach is also being advocated by MSG-ET-044 [2] at the physical level for serious game development. In order for this to be cost effective, increased re-use of configuration data will be required. Thus, it is expected that to facilitate all of these design considerations, common standards for the interoperability of services will need to be developed

In [4] we enhanced the IW engagement model architecture diagram of Figure 1 to show examples of the components, information and effects that are modelled in each layer. In that model (primary) cyber effects, as commonly defined, take place in the communications and information layers, depending upon the particular attack type and resulting cyber effect.

Following feedback from the NMSG 151 workshop, we renamed two of the layers. The communications network layer was renamed the conduit layer to avoid confusing it with the OSI network model for communications [6]. The information layer was renamed the content layer to emphasise its role in providing the semantics for the information or data passed throughout the architecture. Figure 2 shows the enhanced IW engagement model architecture diagram using the new layer names. It contains examples of the components, information and effects in each layer.

In preparation for the current work, the architecture of Figure 1 was revisited in light of the work by

Kearse [3] and one issue that was not explicit was that of the difference between simulation truth and simulated entity knowledge. Many lower fidelity simulation model architectures combine truth data, often represented as internal simulation data, and perceived data, which is the state of the world as sensed and understood by the entities modelled in the simulation. Perceived data and truth data are distinct concepts, while equating truth and perceived data within a simulation can be a valid modelling technique for particular levels of fidelity it is particularly constraining when modelling warfare techniques that directly target the perceived data. A more flexible and maintainable design stores them separately, even if they are equated in an initial implementation, so that they can be distinguished later when the need arises. In Figure 2 we have added links from the physical layer to the content and conduit layers to indicate the storage of simulation truth data within the architecture. Perceived data is generated via sensor reports that move through the conduit layer to content or cognition layers for storage or use.

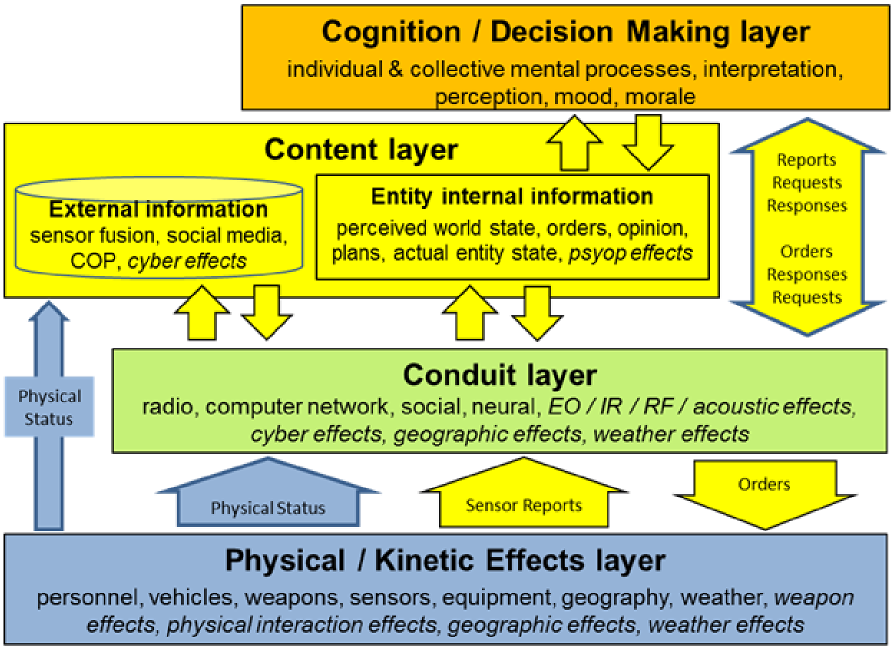
Cognition / Decision Making layer
individual & collective mental processes, interpretation, perception, mood, morale
Content layer
External information
sensor fusion, social media, COP, cyber effects
Entity internal information
perceived world state, orders, opinion, plans, actual entity state, psyop effects
Reports
Requests
Responses
Orders
Responses
Requests
Physical Status
Conduit layer
radio, computer network, social, neural, EO / IR / RF / acoustic effects, cyber effects, geographic effects, weather effects
Physical Status
Sensor Reports
Orders
Physical / Kinetic Effects layer
personnel, vehicles, weapons, sensors, equipment, geography, weather, weapon effects, physical interaction effects, geographic effects, weather effects

Figure 2: Information Warfare engagement model architecture showing the location of (primary) cyber effects.

While our primary use for this IW engagement model architecture is to propose extensions to CGF architectures to support IW, which are by definition constructive, the architecture is applicable to Live, Virtual and Constructive (LVC) simulation. For example, a blue force decision-making participant in a simulation is conceptually located in the cognition layer in the same way as an agent-based red force opponent behavioural model.

LAYER FUNCTIONALITY AND DATA MODEL INVESTIGATION: USE CASE ANALYSIS

The analysis of the architecture in this paper is based on a general use-case of *training of naval staff officers in information warfare*. Within this use-case the naval staff generates an operations plan that includes the use of offensive cyber operations and the supporting CGF must be able to simulate the operations and results. The use case was analysed as a sequence of steps (shown in Table 1) as suggested by Fowler [7].

Step	Use-Case Step Description
1	CTG Staff prepares an OCO plan consisting of the following steps: 1. Use social media to encourage Adversary to choose a route that the TG can intercept 2. Infiltrate Adversary cell phones and/or laptops to confirm location in port and monitor adversary planning and execution; e-mail addresses have been supplied by HUMINT 3. Disable Adversary cell phones just prior to interception
2	CTG Staff sends the OCO plan to Subordinate Unit (IW Resources) via e-mail
3	IW Resources review the OCO plan, applying their own opinions and cognitive biases to the interpretation
4	IW Resources seek clarification from CTG Staff on the type of social media, the nature of the cyber attack, the effect to be achieved, and the type of cell phones and laptops as identified by HUMINT via electronic chat
5	CTG Staff clarifies the OCO plan via electronic chat: they have no preference with respect to the type of social media or the nature of cyber attack, but they do want to have as much advanced warning of the Adversary's movements as possible to facilitate interception; CTG Staff also provides the type of cell phones and laptops identified by HUMINT
6	IW Resources decide to use Facebook, Twitter and Instagram, using different aliases, and to try spear-phishing based on HUMINT
7	IW Resources post several messages to Facebook and Twitter using different aliases indicating the TG is in a particular area (that it is not)
8	IW Resources post pictures of the TG with incorrect geotags to Twitter and Instagram using different aliases indicating that the TG is in the same area (that it is not)
9	Adversary sees the messages and pictures and, taking their own opinions and cognitive biases into account, decides to stay away from the indicated area
10	IW Resources prepare and send spear-phishing e-mail directed at the Adversary, and report to CTG Staff that e-mail has been sent
11	Adversary receives spear-phishing e-mail on cell phone, opens the spear-phishing e-mail, and clicks on the spear-phishing link and goes to web site #1 containing malware
12	Malware installs on the Adversary's cell phone, then connects to web site #2 and reports Adversary's position; Adversary's anti-virus software does not detect the presence or actions of the Malware
13	IW Resources check web site #2 and report to CTG Staff via e-mail that the Malware has been successfully installed on Adversary's phone and report Adversary's position as reported by Malware
14	Adversary uses cell phone to plan human smuggling operation; Malware copies message data sent and received (SMS, e-mail, Signal) and voice recordings to web site #2
15	IW Resources monitor web site #2 and reports plans of the Adversary to CTG Staff via e-mail
16	Adversary departs port on a human smuggling operation; Malware connects to web site #2 and reports Adversary's position
17	IW Resources monitor web site #2 and report departure of the Adversary to CTG Staff via e-mail
18	CTG Staff orders TG to sail to intercept Adversary
19	IW Resources command Malware to disable Adversary cell phone; Malware disables Adversary cell phone
20	When in detection range, TG detect then track Adversary by radar then EO/IR then visual
21	TG intercepts Adversary and the training scenario concludes
22	Training Instructor analyses data recorded during the scenario and provides after-action review feedback to the trainee Maritime Staff Officers

Table 1: Steps of the Offensive Cyber Operation Use Case

ANALYSIS

For the purposes of discussing the analysis in this paper, we concentrate on steps 2, 9 and 14 of the use case. Step 2 is an example of communication between the (human) CTG Staff and the (constructive) IW Resources via e-mail. Step 9 is an example of cognition using both external and internal content sources, including cognitive biases. Step 14 contains an example of malware intercepting and communicating content.

In our analysis of the use case and the IW engagement model architecture, we commenced by considering the following aspects: which layer(s) of the IW engagement model architecture does each component and effect in the use case impact; and, how do the operational systems and activities manifest themselves as interfaces between the four layers of the IW engagement model architecture.

Layer Effects

Table 2 contains examples of the effects that can influence components in each of the different layers in the IW engagement model architecture. Within the use case, the most relevant effects are cyber effects, in the use of malware, and psychological operations, in the use of social media to influence the Adversary.

Effects	Physical	Conduit	Content	Cognition
Weapon	Primary	Secondary	Secondary & Tertiary	Tertiary
Physical Interactions	Primary	Secondary	Secondary & Tertiary	Tertiary
Geographic	Primary	Primary	Secondary	Tertiary
Weather	Primary	Primary	Secondary	Tertiary
EO / IR / RF / Acoustic	Tertiary & Secondary	Primary	Secondary	Tertiary
Cyber	Tertiary & Secondary	Primary & Secondary	Primary	Secondary, Tertiary & Primary
Psychological Operations	Tertiary	Tertiary	Primary	Secondary

Table 2: Effects modelling within the IW engagement model architecture

We provided details of how the different types of cyber effects can affect each layer in [3]. One addition in Table 2 compared to [3] is that we now consider that primary effects can also be realised in the cognition layer, in addition to the conduit and content layers. This is because we now consider that the cognition layer encompasses current or future computer and information systems that can be regarded as “decision makers”. These systems are susceptible to cyber attack in the same way that computer, information and network systems in the conduit and content layers are, and so primary cyber effects can affect the cognition layer. As most computer, information and network systems in the conduit and content layers support human decision makers, it remains that secondary and tertiary effects in the cognition layer will be the most common result from cyber attacks.

Psychological operations aim to influence the behaviour of humans, individually or in groups, and their decision making through the provision of information content that creates an affective contribution to decision making (e.g., morale, hope, affinity) that is advantageous to the initiator's objective. As such, psychological operations effects primarily occur in the content layer, and target shaping the entity's internal information in the IW engagement model architecture. Secondary effects occur in the cognition layer because of the shaped information, resulting in altered decision making. The decisions result in tertiary effects in the conduit and physical layers.

Mapping of Operational Systems to Architecture Layers

Our initial aim with the use case was to assist in understanding how the operational systems of the use case may relate to the layers of the IW engagement model architecture. To achieve this, we extracted each of the operational systems and relevant key pieces of information that were either explicitly referenced or implied from the steps of the use case and mapped their constituent conceptual elements that we would expect to model to the four layers of the architecture.

Table 3 contains an example subset of the resultant mapping of operational systems and key information of the use case to the layers of the IW engagement model architecture. When an operational system appears in a layer, we provide an example of the role that the system plays or the data that it encapsulates in that layer. Table 3 also shows whether a live (L), virtual (V) or constructive (C) component is generally used to simulate each system in the use case.

Operational System	LVC	Physical	Conduit	Content	Cognition
CTG Staff	L	Location		Knowledge	Decision making
IW Resources staff	C	Location		Entity internal information	Decision making
CTG Staff computers	L or V	Location	Network node & processing	Processing & storage	
Twitter web service	C		Web service	Web content	
Instagram web service	C		Web service	Web content	
Twitter content	C		Transport	Data	
Instagram content	C		Transport	Data	
Cell phone network	C	Locations	Nodes & connections	Configuration	
Internet	C	Locations	Nodes & connections	Configuration	

Table 3: Representative mapping of operational systems to architecture layers implied by the use case

As Table 3 focusses on the use case, it does not guarantee that all possible mappings of systems to layers are covered. For example, a model of a human, such as IW Resources staff, may explicitly belong in the conduit layer for direct verbal communication with no intervening technology. However, there is no such step in the use case so this representation does not appear in Table 3.

Architecture Layer Interfaces

Our next step was to decompose each step in the use case into a sequence of the operational systems, identified in the previous mapping, and activities performed by the operational systems. Each sequence was then used to construct a UML communication diagram for the use case step to identify the communication occurring between components, and the functions and parameters involved.

Table 4 shows the resulting decomposition for step 2 of the use case into a sequence of steps involving the operational systems and key information. Some of the operational systems, such as the CTG Staff and IW Resources, were referenced directly in the use case step, while others, such as the CTG Staff computer and TG Network, are implied by the modelling required to implement the activity. Similarly, some of the key information, such as the OCO plan, was referenced directly in the use case step, while others, such as CTG Staff e-mail content, were implied.

The sequence shown in Table 4 is representative of many of the steps of the use case that involve computer-based communications systems, such as e-mail and chat, and shows the transmission of content across multiple computer networks. It shows that most of the operational systems involved in this step are considered to be part of the conduit layer, with only a few in each of the other three layers.

Figure 3 shows the resulting UML communication diagram for step 2 of the use case derived from the information in Table 4. The components in each of the four different layers are shown using a different colour: green for physical, yellow for conduit, light orange for content and dark orange for cognition. In addition, the blocks of messages in Figure 3 corresponding to each block of steps in Table 4 are shown in different colours. As for Table 4, Figure 3 is representative of the communication diagrams for many steps of the use case that involve computer-based communications systems.

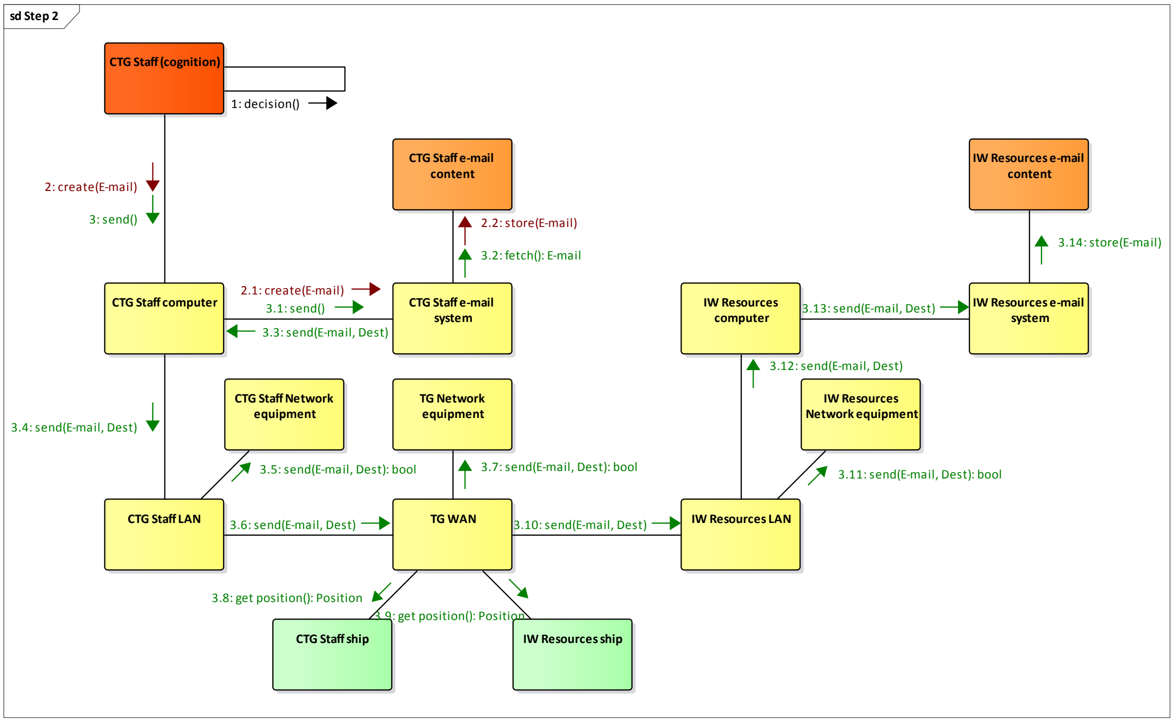

Figure 3: Communication diagram for step 2 of the use case

Operation System and activity	**Role Type**	**Layer**
CTG Staff decide to send e-mail	Decision	Cognition
containing *OCO plan*	Information	Content
CTG Staff create e-mail	Action	Cognition
using *CTG Staff computer*	Communication System	Conduit
and *CTG Staff e-mail system*,	Communication System	Conduit
it is stored as *CTG Staff e-mail content*	Information	Content
CTG Staff sends created e-mail to addressee	Action	Cognition
using *CTG Staff e-mail system*	Communication System	Conduit
on the *CTG Staff computer*;	Communication System	Conduit
CTG Staff e-mail system sends e-mail	Communication System	Conduit
from *CTG Staff e-mail content*	Information	Content
routing it over *CTG Staff LAN*	Communication System	Conduit
which uses *CTG Staff Network* equipment,	Communication System	Conduit
TG WAN	Communication System	Conduit
which uses *TG Network* equipment	Communication System	Conduit
and uses *CTG Staff ship* and *IW Resources ship* locations,	Location	Physical
IW Resources LAN	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
to the *IW Resources e-mail system*	Communication System	Conduit
on the *IW Resources computer*,	Communication System	Conduit
the e-mail is stored as *IW Resources e-mail content*	Information	Content

Table 4: Operational systems and activities in step 2 of the use case

Table 5 shows the resulting decomposition for step 9 of the use case into a sequence of steps involving the operational systems and key information referenced directly and implied by the use case step. The sequence shown in Table 5 is representative of the steps of the use case that involve the use of internet-based social media and cell phone “apps” for communication. Notably, it also demonstrates a form of psychological operations: social media content previously planted by the IW Resources (in earlier steps) combine with the opinions and cognitive biases of the Adversary to affect the decision making of the Adversary.

Operation System and activity	**Type**	**Layer**
Adversary uses	Action	Cognition
the *Facebook app*	Communication System	Conduit
on an *Adversary cell phone*	Communication System	Conduit
to view *Facebook content*	Information	Content
which is sent via the *Cell phone network*	Communication System	Conduit
taking the *Adversary cell phone* location into account	Location	Physical
and the *Internet*,	Communication System	Conduit
from the *Facebook web service*	Communication System	Conduit
which stores each message as *Facebook content*	Information	Content
Adversary uses	Action	Cognition
the *Twitter app*	Communication System	Conduit
on an *Adversary cell phone*	Communication System	Conduit
to view *Twitter content*	Information	Content
which is sent via the *Cell phone network*	Communication System	Conduit
taking the *Adversary cell phone* location into account	Location	Physical
and the *Internet*,	Communication System	Conduit
from the *Twitter web service*	Communication System	Conduit
which stores each message as *Twitter content*	Information	Content
Adversary uses	Action	Cognition
the *Instagram app*	Communication System	Conduit
on an *Adversary cell phone*	Communication System	Conduit
to view *Instagram content*	Information	Content
which is sent via the *Cell phone network*	Communication System	Conduit
taking the *Adversary cell phone* location into account	Location	Physical
and the *Internet*,	Communication System	Conduit
from the *Instagram web service*	Communication System	Conduit
which stores each message as *Instagram content*	Information	Content
Adversary decides to stay away from an area	Decision	Cognition
based on the *Facebook content*,	Information	Content
Twitter content	Information	Content
and *Instagram content*	Information	Content
in the context of their opinions and cognitive biases	Information	Content

Table 5: Operational systems and activities in step 9 of the use case

Figure 4 shows the resulting UML communication diagram for step 9 of the use case derived from the information in Table 5. It explicitly shows the Adversary cognition component retrieving cognitive biases and opinions from the Adversary content component: the internal entity information.

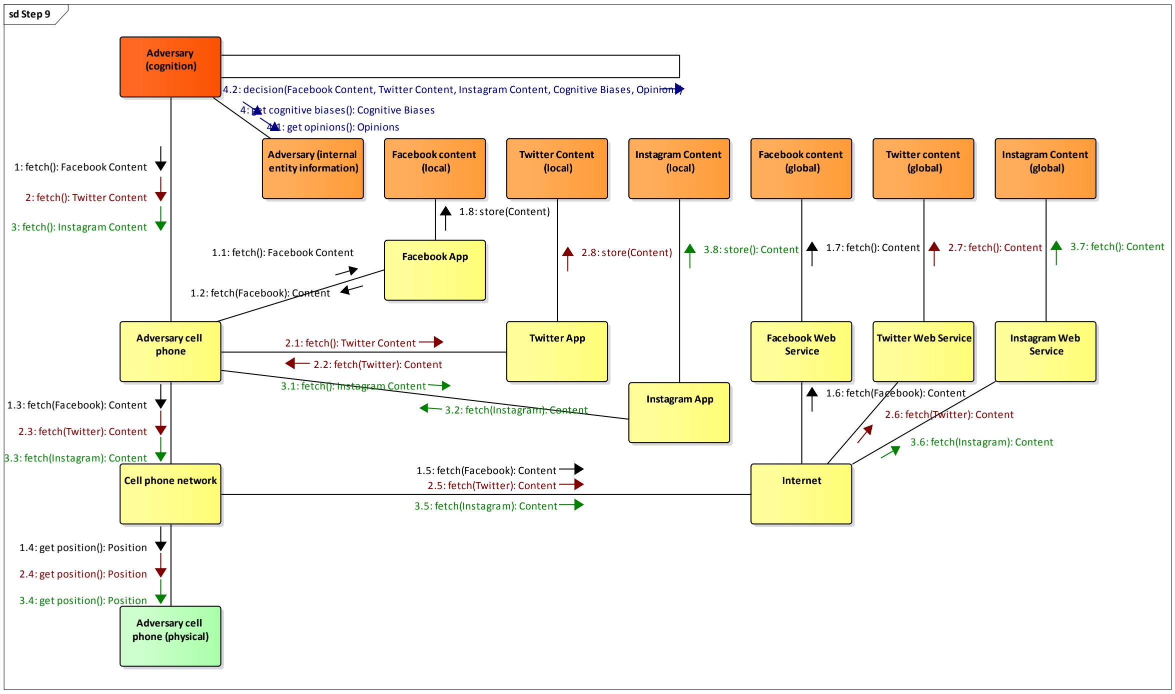
sd Step 9
Adversary (cognition)
4.2: decision(Facebook Content, Twitter Content, Instagram Content, Cognitive Biases, Opinion)
4: get cognitive biases(): Cognitive Biases
4.1: get opinions(): Opinions
Adversary (internal entity information)
Facebook content (local)
Twitter Content (local)
Instagram Content (local)
Facebook content (global)
Twitter content (global)
Instagram Content (global)
1: fetch(): Facebook Content
2: fetch(): Twitter Content
3: fetch(): Instagram Content
1.8: store(Content)
1.1: fetch(): Facebook Content
1.2: fetch(Facebook): Content
Facebook App
2.8: store(Content)
3.8: store(): Content
1.7: fetch(): Content
2.7: fetch(): Content
3.7: fetch(): Content
Adversary cell phone
2.1: fetch(): Twitter Content
2.2: fetch(Twitter): Content
3.1: fetch(): Instagram Content
3.2: fetch(Instagram): Content
Twitter App
Instagram App
Facebook Web Service
Twitter Web Service
Instagram Web Service
1.6: fetch(Facebook): Content
2.6: fetch(Twitter): Content
3.6: fetch(Instagram): Content
1.3: fetch(Facebook): Content
2.3: fetch(Twitter): Content
3.3: fetch(Instagram): Content
Cell phone network
1.5: fetch(Facebook): Content
2.5: fetch(Twitter): Content
3.5: fetch(Instagram): Content
Internet
1.4: get position(): Position
2.4: get position(): Position
3.4: get position(): Position
Adversary cell phone (physical)

Figure 4: Communication diagram for step 9 of the use case

Table 6 shows the resulting decomposition for step 14 of the use case into a sequence of steps involving the operational systems and key information reference directly and implied by the use case step. The sequence shown in Table 6 again shows the use of internet and cell phone communication. Notably, it also demonstrates a form of cyber effect, interception, in that the malware installed during step 12 of the use case intercepts the communications of the Adversary and uploads them to a web site for later download by the IW Resources.

Operation System and activity	**Type**	**Layer**
Adversary	Action	Cognition
uses the *Adversary cell phone*	Communication System	Conduit
which uses the *Cell phone network,*	Communication System	Conduit
which takes the *Adversary cell phone* location into account,	Location	Physical
to send and receive SMS messages to plan the human smuggling operation	Information	Content
Malware	Information System	Content
on the *Adversary cell phone*	Communication System	Conduit
uses the *Adversary Wi-Fi LAN*	Communication System	Conduit
which uses *Adversary Network* equipment	Communication System	Conduit
and takes the *Adversary cell phone* location into account	Location	Physical
and the *Internet*,	Communication System	Conduit
to connect to *Web site #2*	Communication System	Conduit
and upload the SMS message data sent and received	Information	Content
Adversary	Action	Cognition
uses the *Adversary cell phone e-mail client*	Communication System	Conduit
on the *Adversary cell phone*	Communication System	Conduit
which uses the *Adversary Wi-Fi LAN*	Communication System	Conduit
which uses *Adversary Network* equipment	Communication System	Conduit
and takes the *Adversary cell phone* location into account	Location	Physical
and the *Internet*,	Communication System	Conduit
to send and receive e-mail messages to plan the human smuggling operation	Information	Content
Malware	Information System	Content
on the *Adversary cell phone*	Communication System	Conduit
uses the *Adversary Wi-Fi LAN*	Communication System	Conduit
which uses *Adversary Network* equipment	Communication System	Conduit
and takes the *Adversary cell phone* location into account	Location	Physical
and the *Internet*,	Communication System	Conduit
to connect to *Web site #2*	Communication System	Conduit
and upload the e-mail message data sent and received	Information	Content

Adversary	Action	Cognition
uses the *Adversary cell phone Signal client*	Communication System	Conduit
on the *Adversary cell phone*	Communication System	Conduit
which uses the *Adversary Wi-Fi LAN*	Communication System	Conduit
which uses *Adversary Network* equipment	Communication System	Conduit
and takes the *Adversary cell phone* location into account	Location	Physical
and the *Internet*,	Communication System	Conduit
to send and receive messages to plan the human smuggling operation	Information	Content
Malware	Information System	Content
on the *Adversary cell phone*	Communication System	Conduit
uses the *Adversary Wi-Fi LAN*	Communication System	Conduit
which uses *Adversary Network* equipment	Communication System	Conduit
and takes the *Adversary cell phone* location into account	Location	Physical
and the *Internet*,	Communication System	Conduit
to connect to *Web site #2*	Communication System	Conduit
and upload the message data sent and received	Information	Content
Adversary	Action	Cognition
uses the *Adversary cell phone Signal client*	Communication System	Conduit
on the *Adversary cell phone*	Communication System	Conduit
which uses the *Adversary Wi-Fi LAN*	Communication System	Conduit
which uses *Adversary Network* equipment	Communication System	Conduit
and takes the *Adversary cell phone* location into account	Location	Physical
and the *Internet*,	Communication System	Conduit
to make and receive voice calls to plan the human smuggling operation	Information	Content
Malware	Information System	Content
on the *Adversary cell phone*	Communication System	Conduit
uses the *Adversary Wi-Fi LAN*	Communication System	Conduit
which uses *Adversary Network* equipment	Communication System	Conduit
and takes the *Adversary cell phone* location into account	Location	Physical
and the *Internet*,	Communication System	Conduit
to connect to *Web site #2*	Communication System	Conduit
and upload the voice recordings	Information	Content

Table 6: Operational systems and activities in Step 14 of the use case

Figure 5 shows the resulting UML communication diagram for step 14 of the use case derived from the information in Table 6. This diagram contains the greatest number of messages of any of the communication diagrams created for the use case, although many of the messages are similar.

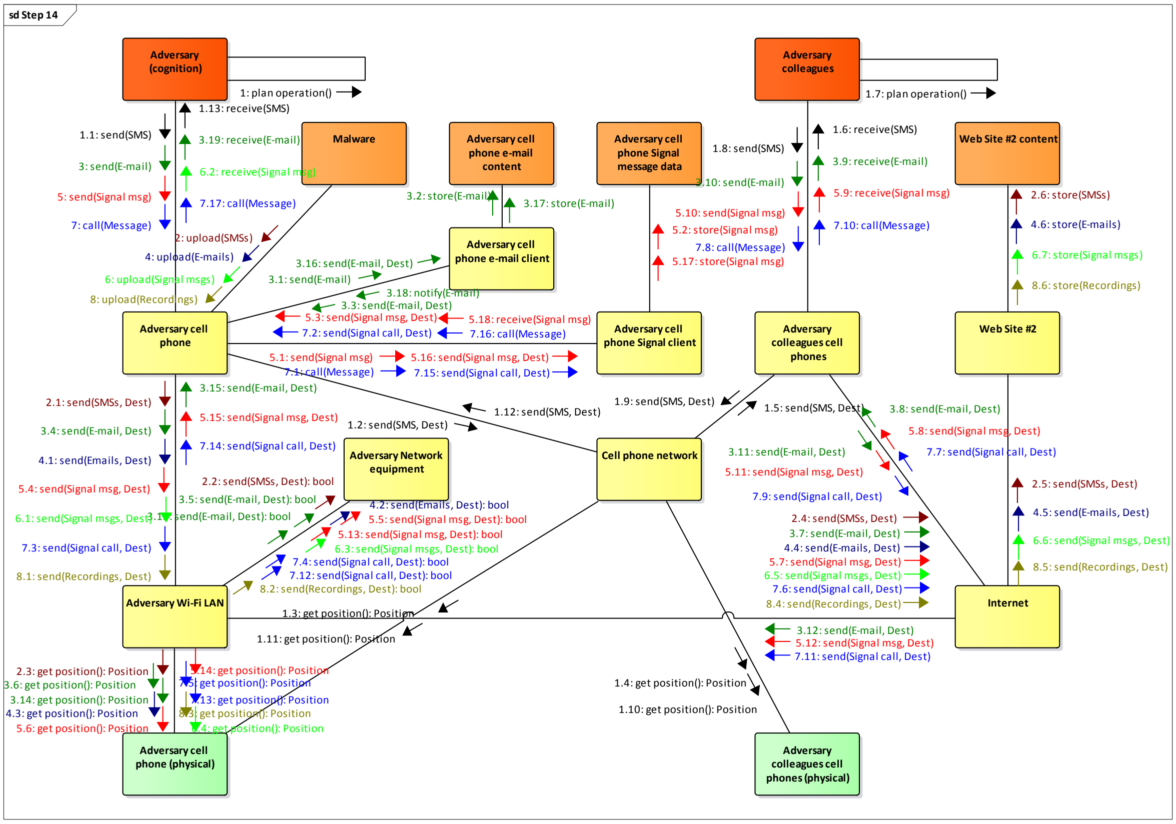
sd Step 14
Adversary (cognition)
1: plan operation()
1.13: receive(SMS)
1.1: send(SMS)
3.19: receive(E-mail)
3: send(E-mail)
6.2: receive(Signal msg)
5: send(Signal msg)
7.17: call(Message)
7: call(Message)
Malware
Adversary cell phone e-mail content
3.2: store(E-mail)
3.17: store(E-mail)
Adversary cell phone Signal message data
Adversary colleagues
1.7: plan operation()
1.8: send(SMS)
1.6: receive(SMS)
3.9: receive(E-mail)
3.10: send(E-mail)
5.9: receive(Signal msg)
5.10: send(Signal msg)
5.2: store(Signal msg)
7.8: call(Message)
5.17: store(Signal msg)
7.10: call(Message)
Web Site #2 content
2.6: store(SMSs)
4.6: store(E-mails)
6.7: store(Signal msgs)
8.6: store(Recordings)
2: upload(SMSs)
4: upload(E-mails)
6: upload(Signal msgs)
8: upload(Recordings)
Adversary cell phone e-mail client
3.16: send(E-mail, Dest)
3.1: send(E-mail)
3.18: notify(E-mail)
3.3: send(E-mail, Dest)
5.3: send(Signal msg, Dest)
5.18: receive(Signal msg)
7.2: send(Signal call, Dest)
7.16: call(Message)
5.1: send(Signal msg)
5.16: send(Signal msg, Dest)
7.1: call(Message)
7.15: send(Signal call, Dest)
Adversary cell phone
Adversary cell phone Signal client
Adversary colleagues cell phones
Web Site #2
3.15: send(E-mail, Dest)
2.1: send(SMSs, Dest)
5.15: send(Signal msg, Dest)
3.4: send(E-mail, Dest)
7.14: send(Signal call, Dest)
4.1: send(Emails, Dest)
5.4: send(Signal msg, Dest)
6.1: send(Signal msgs, Dest)
7.3: send(Signal call, Dest)
8.1: send(Recordings, Dest)
1.12: send(SMS, Dest)
1.2: send(SMS, Dest)
1.9: send(SMS, Dest)
1.5: send(SMS, Dest)
3.8: send(E-mail, Dest)
5.8: send(Signal msg, Dest)
7.7: send(Signal call, Dest)
Adversary Network equipment
Cell phone network
3.11: send(E-mail, Dest)
5.11: send(Signal msg, Dest)
7.9: send(Signal call, Dest)
2.5: send(SMSs, Dest)
4.5: send(E-mails, Dest)
6.6: send(Signal msgs, Dest)
8.5: send(Recordings, Dest)
2.2: send(SMSs, Dest): bool
3.5: send(E-mail, Dest): bool
3.13: send(E-mail, Dest): bool
4.2: send(Emails, Dest): bool
5.5: send(Signal msg, Dest): bool
5.13: send(Signal msg, Dest): bool
6.3: send(Signal msgs, Dest): bool
7.4: send(Signal call, Dest): bool
7.12: send(Signal call, Dest): bool
8.2: send(Recordings, Dest): bool
2.4: send(SMSs, Dest)
3.7: send(E-mail, Dest)
4.4: send(E-mails, Dest)
5.7: send(Signal msg, Dest)
6.5: send(Signal msgs, Dest)
7.6: send(Signal call, Dest)
8.4: send(Recordings, Dest)
Adversary Wi-Fi LAN
Internet
1.3: get position(): Position
1.11: get position(): Position
3.12: send(E-mail, Dest)
5.12: send(Signal msg, Dest)
7.11: send(Signal call, Dest)
2.3: get position(): Position
3.6: get position(): Position
3.14: get position(): Position
4.3: get position(): Position
5.6: get position(): Position
5.14: get position(): Position
7.5: get position(): Position
7.13: get position(): Position
8.3: get position(): Position
6.4: get position(): Position
1.4: get position(): Position
1.10: get position(): Position
Adversary cell phone (physical)
Adversary colleagues cell phones (physical)

Figure 5: Communication diagram for step 14 of the use case

Analysis discussion

The analysis that resulted in the production and use of the UML communication diagrams proved to be a very effective method of understanding the processes involved in each step. Extracting the operational systems and key information from the use case steps enabled us to determine a plausible decomposition of the models that would be required in the simulation. It also showed that the conduit layer plays a critical role in the transportation of information between the various components.

During our analysis, we found that the individual use case steps were at too high a level to directly and reliably produce UML communication diagrams. This led to the production of the operational systems and activities tables that decomposed each use case step into a series of lower level steps with more detailed operational systems than in the use case step. From these, developing UML communication diagrams was significantly easier in terms of being freer of consistency errors.

Notwithstanding the effectiveness of the diagrams, it was time consuming to analyse each step and ensure the consistency of representation between steps. A number of the steps, especially those that involved computer and cell phone originated communications, were common across multiple diagrams. While this validated our analysis and confirmed patterns on one level, on another it did mean that multiple threads of the analysis had the same, or a very similar, outcomes. Fortunately, these patterns [5] will have wider application and so can be used to accelerate similar analyses in future.

DATA MODEL

Following our exploration of the communication between components within and across the architecture layers, our aim was to develop a (high level) data model that represents the use case that can apply to simulation specification and initialisation and at simulation run-time. Rather than directly apply or extend an existing data model, our initial aim was to explore a data model that would naturally flow from our use case and then compare the result with existing military and simulation data models.

Interactions

The interactions that occur in the use case are captured in the UML communication diagrams described above. Here we characterise the connections between the components in terms of the interactions between them and the data used by the interactions.

Table 7 contains a summary of the interactions derived from the use case. Due to the nature of the use case, most of the interactions originate from components in the cognition layer.

Originating Layer	Category	Action type	Example verb
Cognition	Operate	Verbal	Say, call
Cognition	Operate	Physical	Move, watch, type
Cognition	Entity Internal Information	Input	Get, recall, fetch
Cognition	Entity Internal Information	Output	Put, remember, store
Cognition / Content / Conduit	Command	Input	Get, fetch, read, download
Cognition / Content / Conduit	Command	Output	Put, store, write, send
Cognition / Content / Physical	Command	Act	Do, move, navigate, board, detain
Content / Conduit / Physical	Signal	Signal	Alarm, notify
Physical	Sensor	Output	Send track

Table 7: Interactions by layer for the use case

Interactions originating within the cognition layer can be broadly placed into three categories: interactions that *operate* another component, interactions with *entity internal information* that are conceptually part of the same component (e.g., the same human), and interactions that are *commands* to another component. The destination component of *commands* and *operate* interactions may be in any of the other three layers, while interactions with *entity internal information* are always an interaction with the content layer.

Commands that obtain input or produce output (e.g., “get” and “put”) may also originate within the content and conduit layers, and many of the interactions in these layers are of this type. *Commands* to act, such as instructions to execute SOPs, may also originate within the physical layer. This allows basic elements of a CGF to support and execute elements of SOPs without the need to further decompose them into more primitive instructions.

Another type of interaction are those generated by components in the physical, conduit or content layers that are intended to alert or *signal* the cognition layer. In addition, there are interactions that result from specific equipment spontaneously providing data, such as *sensor* output.

Table 8 contains a summary of the interaction parameter and result object data derived from the use case. Note that object data shown in italics are not explicitly referenced in the use case.

Layer	**Subcategory**	**Object Data**
Cognition		Request, Response, Voice message (live) *Morale*
Content	Military C2	Order, Plan, Report *Command hierarchy, battle damage assessment*
	Electronic message	E-mail message, Chat message
	World Wide Web	URL, Web page, Software (malware)
	Social media	Facebook message, Tweet (twitter message), Instagram post
	Cell phone	SMS message, Voice recording
	Entity Internal Information	Opinion, Cognitive biases
Conduit	Status	*Link status, Communications node status, malware status, error status*
Physical	Position	Location
	Sensor	Track

Table 8: Interaction parameter & result object data by layer for the use case

While most of the interactions of the use case are generated by components in the cognition layer, the greatest numbers of types of objects relating to those interactions belong to the content layer. Given the roles played by the two layers, this intuitively makes sense.

Base Simulation Object

In determining features required of the base *Simulation Object*, which is to be the root object for our data model object class hierarchy, we consider that objects derived from it will be used in the simulation at both simulation run-time and during the simulation specification (order of battle (ORBAT), a listing of military units, construction). To facilitate this, we believe that each *Simulation Object* should encapsulate three concepts.

The first concept is that, as discussed above, we believe that there should be an explicit distinction made between truth and perceived data in the object model. This will be useful in developing the simulation and analysing its results, including use in the generation of measures of performance and measures of effectiveness, and in after action review.

The second concept is to assist in simulation scenario specification, in particular. We identify whether each *Simulation Object* belongs to, or is, a live, virtual or constructive simulation component, for the reasons discussed above.

For the third concept, we believe that it may be useful to identify the layer(s) that an object belongs to. This will allow for the establishment and validation of a layer-dependent contract that each object must satisfy or set of base capabilities.

In our data model, we represent these three concepts as enumerations and simple attributes of the base *Simulation Object*. Alternative approaches could use interfaces, methods or abstract methods, or multiple inheritance.

Classes from the Object Model

Here we present some example class hierarchies from the object model derived from the use case.

Figure 6 contains a class diagram documenting the object model class hierarchy associated with messages, derived from *Information* and the base *Simulation Object*. As discussed above, the *Simulation Object* contains attributes identifying the layer(s), LVC type and whether it is perceived or truth data. The use case contains a relatively rich set of message types, including plans, orders and reports associated with military C2 systems, e-mail, web pages and social media service messages associated with the internet, and SMS and voice messages from cell phones. Each of these is represented in the class diagram.

Figure 7 contains a class diagram documenting the object model class hierarchy associated with services and service provision, derived from the base *Simulation Object.* It establishes the relationship between network, internet and cell phone services, the technical systems that provide those services, and the organizations that provide those services in the use case. We expect that each of these will have different properties that will be valuable to specify when a scenario is constructed, and modelled at simulation run-time.

Figure 8 contains a class diagram documenting the object model class hierarchy for interactions, based on the interactions described in Table 7. These classes extend a base *Interaction* class and not *Simulation Object* because interactions represent events and not objects. Note that the classes extending *Command* are not included on this class diagram to maintain legibility.

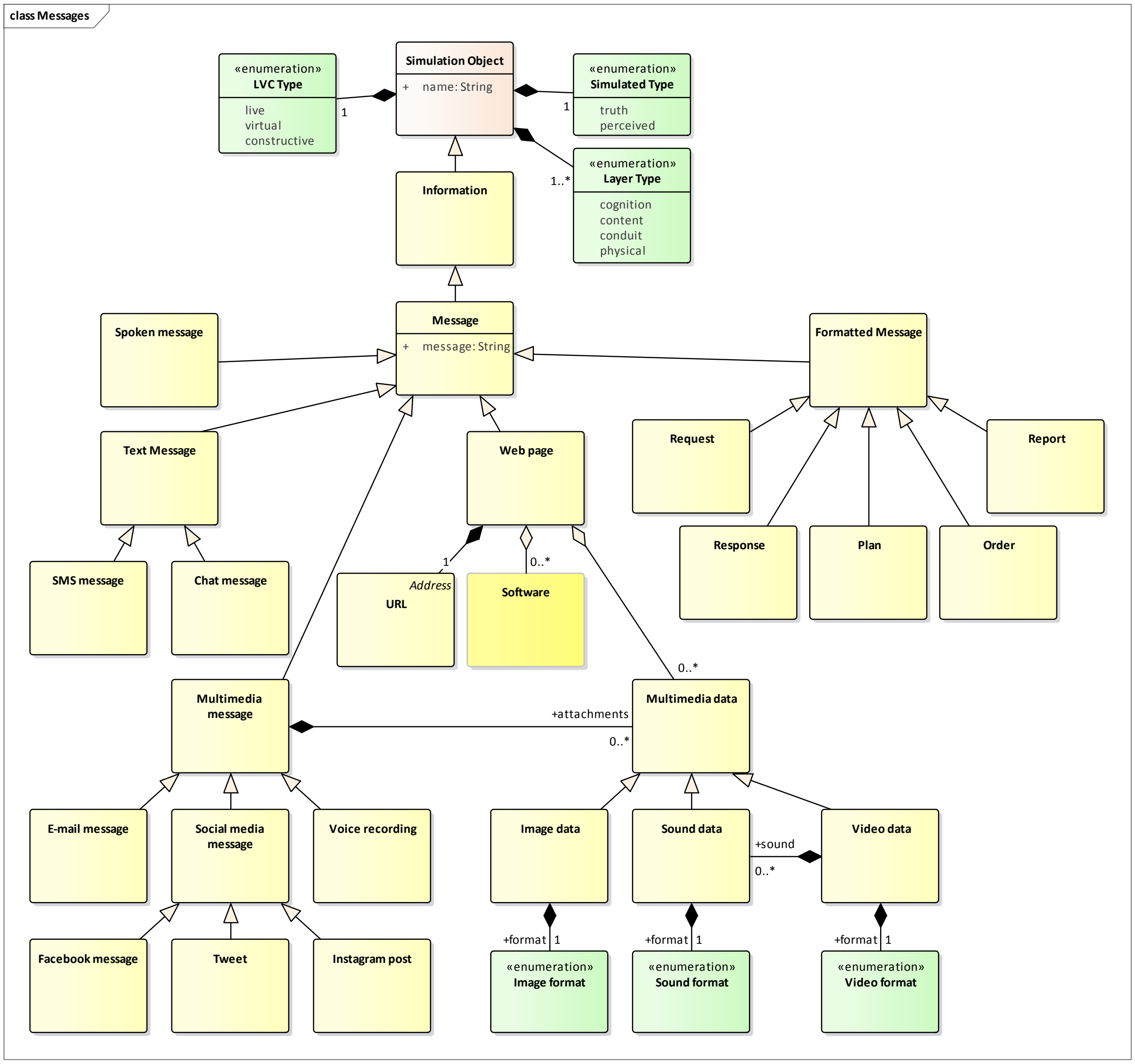

Figure 6: Class diagram for messages

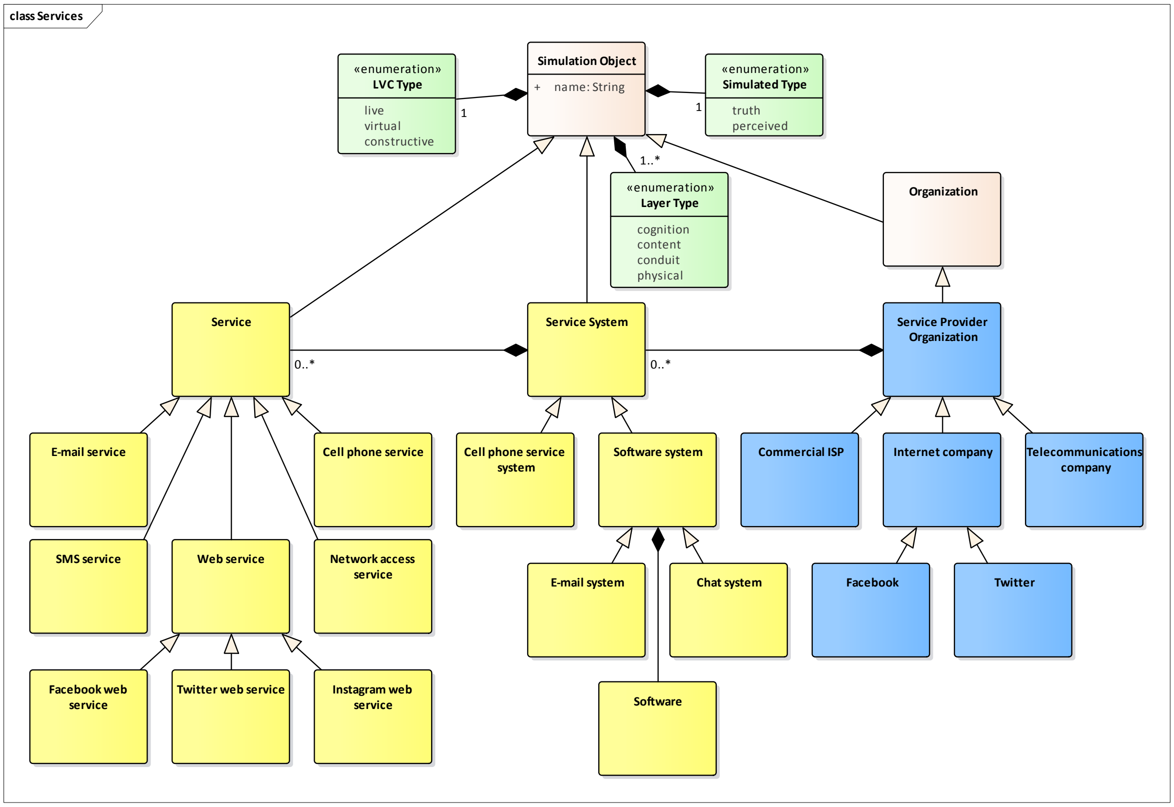

Figure 7: Class diagram for services

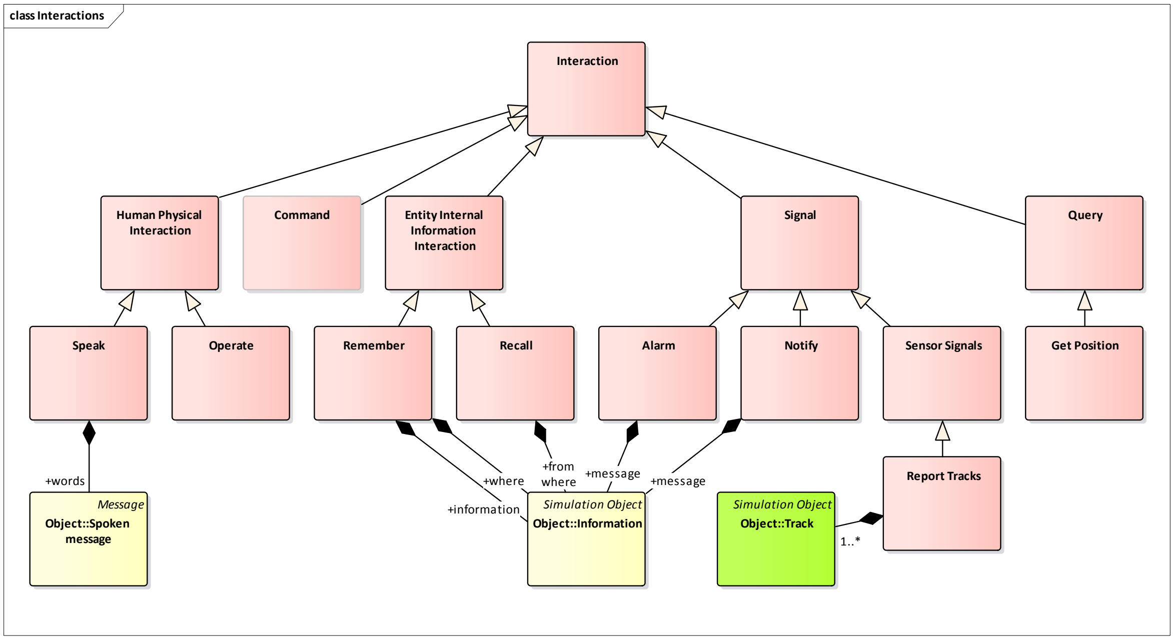

Figure 8: Class diagram for interactions (ex commands)

Other Data Models

In developing our data model, we deliberately did not directly align it with any of the existing (more detailed) military C2 and simulation data models, in the knowledge that the use case covers areas that are currently not well supported by these data models. In areas that do overlap with the use case, they are obviously much more detailed than our data model.

The data model defined by the Distributed Interactive Simulation (DIS) Protocol Data Unit (PDU) standard [8,9] and the equivalent representation for the High Level Architecture (HLA), the Real-time Platform Reference (RPR) Federation Object Model (FOM) [10], is the most commonly used data model for constructive and virtual simulation and is supported by all modern CGFs. The DIS standard defines the precise format of messages exchanged between simulation hosts at run-time, while the HLA RPR FOM defines equivalent message content. These standards only apply at simulation run-time and are not used to define an ORBAT or during simulation initialisation. The DIS 6 PDUs and HLA RPR FOM are largely complementary to our data model because they define messages that belong to the physical and, to a lesser extent, the conduit layer and do not consider the content or cognitive layers at all. In addition, at the conduit layer, the focus of the PDUs is on transmissions and emissions rather than transporting content.

The most recent revision of the DIS standard [11] added additional PDUs for Information Operations (IO): the IO Action PDU and IO Report PDU. While the intent of these PDUs is to support all types of IO, the current representation is limited to communication networks and nodes. As such, they currently only affect the conduit layer of the IW engagement model architecture. To the best of our knowledge, these IO PDUs are not widely supported by existing CGFs.

The Multilateral Information Programme (MIP) Information Model (MIM) [12] is intended to provide a foundation for the real-time exchange of data in the C2 domain. The MIM is a successor to the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) [13]. The primary focus of the MIM is not simulation, although the elements within the data model could be simulated and components using the MIM can be involved in a live simulation. However, from a simulation perspective, it does not represent a complete data model. To the best of our knowledge, neither the JC3IEDM nor the MIM are widely supported by existing CGFs.

When considering the IW engagement model architecture, the MIM defines classes that belong in the physical, conduit and content layers, although the representation is not complete from the perspective of the IW engagement model architecture. The MIM includes a representation of computer and communications hardware, networks and some network services. It also includes classes for plans, orders and reports. However, as its focus is C2 and not simulation, it does not include a representation of decision makers, decision making processes, or how some services in the content and conduit layers, such as computer operating systems or software, may be implemented.

The Coalition Battle Management Language (C-BML) [14] is designed to support the exchange of plans, orders, requests and reports across C2 and LVC M&S systems. Its data model is based on JC3IEDM. As such, C-BML also defines classes that belong in the physical, conduit and content layers, although the representation is not complete from the perspective of the IW engagement model architecture. Again, it does not include a representation of decision makers, decision-making processes, or how some services in the content and conduit layers may be implemented.

The Military Scenario Definition Language (MSDL) [15] is designed to support the development of scenarios used at simulation initialization time. MSDL uses relevant elements from the JC3IEDM as a part of its data type definitions. The MSDL is largely complementary to our data model because it defines elements that belong to the physical and, to a lesser extent, the conduit layers and does not consider elements of the content or cognitive layers to a significant degree. The MSDL provides definitions for units, equipment of the physical layer, and communications nets of the conduit layer. It also provides a definition for overlays that belongs in the content layer.

The Command and Control Systems – Simulation Systems Interoperation (C2SIM) [16] standards activity currently being developed within Simulation Interoperability Standards Organisation (SISO) is intended to effectively merge C-BML and MSDL. In future, it would be beneficial for it to be extended to support additional elements from the IW engagement model architecture.

DISCUSSION AND RECOMMENDATIONS

In our analysis of the use case, we chose to perform a top-down decomposition of the problem. The aim was to assume a level of fidelity and component detail that is appropriate to examine issues that existing CGFs do not support well, or at all, while not expending significant effort on the parts of the architecture that are well supported. Nevertheless, different applications have different modelling fidelity requirements and therefore this work remains a first step.

From an object-oriented design point of view, our analysis shows that many objects/entities exist or have attributes in more than one layer. For example, humans have attributes that result in them being represented in three or four layers in a typical simulation. Additionally, we expect that different use cases will find different demarcation points between modelling decision-maker behaviour, in the cognitive layer using information in the content layer, and automatic behaviour, modelled in the physical and conduit layers. One solution to this, similar to HLA, is to allow object attributes to be "owned" by different services provided by a range of layers. For example, the human entity's physical location attribute could be owned by services in the physical layer, while the internal content is in the content layer and the cognition in the cognitive layer.

Throughout the analysis, it is important to keep an eye on the goal of developing a useful simulation architecture to solve real problems. For the most part, we believe we have been successful, although not without the occasional learning opportunity. For example, our initial decomposition of the physical *operate* interactions in the cognition layer was too deep, to a level that from a practical perspective would not be simulated by a CGF.

The level of decomposition necessary for accurate modelling will always be dependent on the application. For example, decomposing computer systems down to an operating system and individual software applications is likely to be too deep unless cyber operations that attack those systems are being simulated. More work is required to understand which elements need to be simulated for a wider range of cyber operations.

Similarly, the representation of cognitive information, such as opinions and biases, is currently very high level and it is likely that more depth will be needed. Expanding (deepening) the use case is one method of exploring this area, although also examining other use cases is likely to be necessary prior to proposing a general solution.

Aspects of the IW engagement model architecture that are not yet covered in sufficient detail or generality are primarily the upper layers of the architecture. The physical layer is covered well by existing CGFs, and existing communications simulation products and standards cover much of the conduit layer. Within the content layer, military C2 elements are well defined, but other parts of the content layer and the decision layer are not covered well by existing simulation products or standards.

All areas of IW effects can benefit from additional research. Psychological operations are the least well defined and it is likely that significant progress is required before they can be fully modelled and standardised. Cyber operations will also benefit from additional research, in particular, to determine the level of fidelity required to model computer systems for different types of cyber attacks and use cases. While there are high fidelity simulations of EW (EO / IR / RF / acoustic) effects at the systems level, extending this to secondary and tertiary effects applying to the content and cognition layers is another area for future research.

The approach we have taken has successfully identified areas of strength and weakness within existing simulation systems and standards. To extend our data model to the same level of detail as existing data models, such as MIM, C-BML or MSDL, we believe that a prototype implementation of this or another use case would be a valuable next step. It would enable validation of our results and exploration of the engineering issues raised in greater depth.

CONCLUSIONS

The work reported here is the first step in validating the IW engagement model architecture following a use-case based approach. It led to the renaming of two of the layers, and a refinement of their definitions, an examination of the interfaces between the four layers of the architecture, and proposing a high level data model that captures elements of the cognition and content layers not well supported by existing data models. As such, the use-case analysis process described should provide a good initial structure for further investigation of the architecture. No major flaws in the IW engagement model architecture were identified.

In reviewing the data models of existing standards, we find that the physical and conduit layers are generally represented well in a military context. However, coverage of the content layer is limited to formatted information, such as military messages, and some business rules, such as military organizational structure and rules of engagement. The cognition layer is essentially absent from the data models of existing simulation products and standards. We believe that more research is needed on the requirements of cognition and behaviour to better understand the representational needs in areas such as bias, opinion and morale prior to their representation in the content or cognition layers.

In implementing the IW engagement model architecture, we believe that it is important to distinguish between truth and perceived data for each simulation object in order to maintain the integrity of the information and assist in simulation analysis and after action review. To examine such engineering issues in more detail, extend our data model to the same level of detail as existing data models, and to validate our initial results, it is recommended that the next step be a prototype implementation of the architecture based on at least one use case.

REFERENCES

[1] Hazen, M., Lloyd, J. and Harris, E. The Evolution of CGF Architectures to Support Information Warfare Effects. Proceedings of the 2016 NATO Modelling and Simulation Group

Symposium (NMSG 143), Paper 6. October 2016, Budapest Romania. DRDC-RDDC-2016-N040.

[2] NMSG-Exploratory Team 044. Recommendations for Modular Game Architectures. STO-TR-ET-044. 2017 (in Press) www.sto.nato.int.

[3] Kearse, J. Development of a conceptual model to support info/cyber warfare effects in M&S. Proceedings of NATO Modelling and Simulation Group Workshop (NMSG) 151 – Cyber Effects in Campaign and Mission Simulations, Paper 7. 18 July 2017, Portsmouth, UK. (in Press)

[4] Hazen, M., Harris, E. and Lamoureux, T. Extending Computer Generated Forces (CGF) Architectures to Support Information Warfare and Cyber Effects. Proceedings of NATO Modelling and Simulation Group Workshop (NMSG) 151 – Cyber Effects in Campaign and Mission Simulations, Paper 2. 18 July 2017, Portsmouth, UK. (in Press)

[5] Harris, E. and Lamoureux, T. Information Warfare Simulation Architecture Development Task Report. Contract Report, October 2017. (in Press).

[6] ISO/IEC. ISO/IEC 7498-1: Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. 2nd ed. 1994.

[7] Fowler, M. UML Distilled: A Brief Guide to the Standard Object Modeling Language. 2nd ed. Addison-Wesley, 1999.

[8] IEEE. IEEE Std 1278.1-1995: IEEE Standard for Distributed Interactive Simulation – Application Protocols. 1995.

[9] IEEE. IEEE Std 1278.1a-1998: IEEE Standard for Distributed Interactive Simulation – Application Protocols. 1998.

[10] SISO. SISO-STD-001.1-2015: Standard for Real-time Platform Reference Federation Object Model (RPR FOM), Version 2.0. 2015.

[11] IEEE. IEEE Std 1278.1-2012: IEEE Standard for Distributed Interactive Simulation – Application Protocols. 2012.

[12] MIP. MIP Information Model (MIM) – Version 4.1. 2017.

[13] MIP. The Joint C3 Information Exchange Data Model (JC3IEDM Main). 2012.

[14] SISO. SISO-STD-011-2014: Standard for Coalition Battle Management Language (C-BML) Phase 1. 2014.

[15] SISO. SISO-STD-007-2008: Standard for Military Scenario Definition Language (MSDL). 2008.

[16] SISO. C2SIM PDG/PSG - Command And Control Systems - Simulation Systems Interoperation. https://www.sisostds.org/StandardsActivities/DevelopmentGroups/C2SIMPDGPSG-CommandandControlSystems.aspx. Retrieved August 3, 2017.