Defence Research and Development Canada
Recherche et développement pour la défense Canada

DRDC | RDDC
technologysciencetechnologie

Information Warfare Simulation Architecture Development: Task Report

Evan Harris

Tab Lamoureux

Prepared by:
CAE
350 Leggat Dr, Suite 200,
Ottawa, On, Canada,
K2K 2W7

PSPC Contract Number: W7719-155268/001/TOR Task12
Technical Authority: Mark G. Hazen
Contractor's date of publication: October 2017

Defence Research and Development Canada

Contract Report
DRDC-RDDC-2017-C278
November 2017

Canada

IMPORTANT INFORMATIVE STATEMENTS

The information contained herein is proprietary to Her Majesty and is provided to the recipient on the understanding that it will be used for information and evaluation purposes only. Any commercial use including use for manufacture is prohibited.

Disclaimer: This document is not published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada, but is to be catalogued in the Canadian Defence Information System (CANDIS), the national repository for Defence S&T documents. Her Majesty the Queen in Right of Canada (Department of National Defence) makes no representations or warranties, expressed or implied, of any kind whatsoever, and assumes no liability for the accuracy, reliability, completeness, currency or usefulness of any information, product, process or material included in this document. Nothing in this document should be interpreted as an endorsement for the specific use of any tool, technique or process examined in it. Any reliance on, or use of, any information, product, process or material included in this document is at the sole risk of the person so using it or relying on it. Canada does not assume any liability in respect of any damages or losses arising out of or in connection with the use of, or reliance on, any information, product, process or material included in this document.

This document was reviewed for Controlled Goods by Defence Research and Development Canada (DRDC) using the Schedule to the *Defence Production Act*.

CAE Inc.

350 Leggett Drive Suite 200
Ottawa, ON, Canada K2K 2W7
Tel: 613-247-0342
Fax: 613-271-0963

HUMAN FACTORS RESEARCH AND MODELLING TASK 12
INFORMATION WARFARE SIMULATION ARCHITECTURE DEVELOPMENT
TASK REPORT

CONTRACT #: W7719-155268/001/TOR

FOR

DEFENCE RESEARCH AND DEVELOPMENT CANADA
ATLANTIC RESEARCH CENTRE

9 Grove St, Dartmouth, Nova Scotia, B3A 3C5

27 October 2017

Document No. 115088-001 Version 01

APPROVAL SHEET

Document No. 115088-001 Version 01

Document Name: Human Factors Research and Modelling Task 12 Information Warfare Simulation Architecture Development
Task Report

Primary Author

Name **Evan Harris**

Position Senior Modelling & Simulation Consultant, Defence & Security, CAE Canada

Contributing Author

Name **Tab Lamoureux**

Position Senior Consultant, Human Factors, Defence & Security, CAE Canada

Reviewer

Name **Michael Lepard**

Position Senior Modelling & Simulation Consultant, Defence & Security, CAE Canada

Approval

Name **Edward Skinner**

Position Project Manager, Defence & Security, CAE Canada

REVISION HISTORY

Revision	Reason for Change	Origin Date
Version 01 DRAFT A	Draft Use Case section issued.	26 May 2017
Version 01 DRAFT B	Draft Architecture Functionality section issued.	13 June 2017
Version 01 DRAFT C	Draft Architecture Layer Interfaces section issued.	05 July 2017
Version 01 DRAFT D	Draft Data Model section issued.	04 August 2017
Version 01 DRAFT E	First complete draft issued.	13 September 2017
Version 01 DRAFT F	Revised to address review comments.	20 October 2017
Version 01	Report issued	27 October 2017

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND DEFINITIONS

ACINT	ACOUSTIC INTELLIGENCE
AIS	AUTOMATIC IDENTIFICATION SYSTEM
API	APPLICATION PROGRAMMING INTERFACE
AV	ANTI-VIRUS
BDI	BELIEF-DESIRE-INTENTION
C-BML	COALITION BATTLE MANAGEMENT LANGUAGE
C2	COMMAND AND CONTROL
C2SIM	COMMAND AND CONTROL SYSTEMS – SIMULATION SYSTEMS INTEROPERATION
C4ISR	COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE
CAE	CAE INC.
CAL	CALIBER
CEMA	CYBER-ELECTROMAGNETIC ACTIVITIES
CGF	COMPUTER GENERATED FORCES
CIS	COMMUNICATIONS AND INFORMATION SYSTEMS
CNE	COMPUTER NETWORK EXPLOITATION
COMINT	COMMUNICATIONS INTELLIGENCE
COP	COMMON OPERATING PICTURE
COTS	COMMERCIAL OFF-THE-SHELF
CTG	COMMANDER OF THE TASK GROUP
DCO	DEFENSIVE CYBER OPERATIONS
DHCP	DYNAMIC HOST CONFIGURATION PROTOCOL
DIS	DISTRIBUTED INTERACTIVE SIMULATION
DNS	DOMAIN NAME SYSTEM
DOS	DENIAL OF SERVICE
DRDC	DEFENCE RESEARCH AND DEVELOPMENT CANADA
DSL	DIGITAL SUBSCRIBER LINE
EA	ELECTRONIC ATTACK
ELINT	ELECTRONIC INTELLIGENCE
EO	ELECTRO-OPTICAL
EOIR	ELECTRO-OPTICAL INFRARED
EP	ELECTRONIC PROTECTION
ES	ELECTRONIC WARFARE SUPPORT
EW	ELECTRONIC WARFARE
FDDI	FIBER DISTRIBUTED DATA INTERFACE
FOM	FEDERATION OBJECT MODEL

FTP	File Transfer Protocol
HLA	High Level Architecture
HTTP	Hypertext Transfer Protocol
HUMINT	Human Intelligence
ICMP	Internet Control Message Protocol
IDM	Internal Defensive Measures
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IO	Information Operations
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR	Infrared
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISR	Intelligence, Surveillance and Reconnaissance
IST	Information Systems Technology Panel
IW	Information Warfare
IWSA	Information Warfare Simulation Architecture
IWSDM	Information Warfare Simulation Data Model
JC3IEDM	Joint Consultation, Command and Control Information Exchange Data Model
LAN	Local Area Network
LVC	Live, Virtual and Constructive
MAC	Media Access Control
M&S	Modelling And Simulation
MDA	Maritime Domain Awareness
MG	Machine Gun
MIME	Multipurpose Internet Mail Extensions
MIM	MIP Information Model
MIO	Maritime Interdiction Operation
MIP	Multilateral Interoperability Programme
MIW	Maritime Information Warfare
MPEG	Motion Picture Experts Group
MSDL	Military Scenario Definition Language
NATO	North Atlantic Treaty Organization

NFS	NETWORK FILE SYSTEM
NMSG	NATO MODELLING AND SIMULATION GROUP
NNTP	NETWORK NEWS TRANSFER PROTOCOL
NTP	NETWORK TIME PROTOCOL
OCO	OFFENSIVE CYBER OPERATIONS
OODA	OBSERVE, ORIENT, DECIDE, ACT
OP	OPERATION
ORBAT	ORDER OF BATTLE
OSI	OPEN SYSTEMS INTERCONNECTION
OTG	OVER-THE-HORIZON TARGETING GOLD
OTH	OVER-THE-HORIZON
PDU	PROTOCOL DATA UNIT
PHP	PHP: HYPERTEXT PREPROCESSOR
PPP	POINT-TO-POINT PROTOCOL
PSPC	PUBLIC SERVICES AND PROCUREMENT CANADA
PSYOP	PSYCHOLOGICAL OPERATIONS
RA	RESPONSE ACTIONS
RCN	ROYAL CANADIAN NAVY
RF	RADIO FREQUENCY
RFC	REQUEST FOR COMMENTS
RJ45	REGISTERED JACK 45
ROE	RULES OF ENGAGEMENT
RPR	REAL-TIME PLATFORM REFERENCE
RS-232C	RECOMMENDED STANDARD 232 REVISION C
RTI	RUN-TIME INFRASTRUCTURE
SAAS	SOFTWARE AS A SERVICE
SATCOM	SATELLITE COMMUNICATIONS
SIGINT	SIGNALS INTELLIGENCE
SISO	SIMULATION INTEROPERABILITY STANDARDS ORGANIZATION
SME	SUBJECT MATTER EXPERT
SMTP	SIMPLE MAIL TRANSFER PROTOCOL
SMS	SHORT MESSAGE SERVICE
SOA	SERVICE ORIENTED ARCHITECTURE
SOP	STANDARD OPERATING PROCEDURE
SOW	STATEMENT OF WORK
SQL	STRUCTURED QUERY LANGUAGE
SSL	SECURE SOCKETS LAYER
TA	TECHNICAL AUTHORITY
TCP	TRANSMISSION CONTROL PROTOCOL
TG	TASK GROUP
TLS	TRANSPORT LAYER SECURITY
TTPS	TACTICS, TECHNIQUES AND PROCEDURES

TV	TELEVISION
UDP	USER DATAGRAM PROTOCOL
UML	UNIFIED MODELING LANGUAGE
URL	UNIFORM RESOURCE LOCATOR
US	UNITED STATES
V&V	VERIFICATION AND VALIDATION
VMF	VARIABLE MESSAGE FORMAT
VOI	VESSEL OF INTEREST
WAN	WIDE AREA NETWORK
XML	EXTENSIBLE MARKUP LANGUAGE
XSS	CROSS-SITE SCRIPTING

EXECUTIVE SUMMARY

CAE Inc. (CAE) was contracted (Solicitation No. #W7719-155268/001/TOR) by Defence Research and Development Canada (DRDC) – Atlantic Research Centre to implement a number of recommendations that resulted from a multi-national workshop on issues relating to adding an information layer to legacy computer generated forces (CGF) simulations to move towards a standard architecture for information warfare. The recommendations included using use cases as the driver for future investigations. This is the resulting task report.

The first outcome of this task was a use case for a training simulation for naval staff officers that encapsulates multiple areas of information warfare (IW): the use of a cyber attack and electronic warfare (EW) on an adversary to achieve a mission objective. The use case enabled the architecture that resulted from the multi-national workshop to be investigated in more depth.

The architecture was investigated and expanded, including renaming two of the layers of the architecture, and defining more concretely the elements that belong in each layer. Elements of the use case were linked to the architecture to provide a detailed example.

Each step in the use case was then analysed to identify the types of activities and systems involved, and the architectural layers that they belong to. UML communication diagrams were used to document the communication between the elements.

A sample data model was then created by analysing the components in the use case, and the interactions between components and the objects passed in those interactions. The result was compared with existing data models in the command and control (C2) and simulation domains.

CAE believes that the use case analysis process described herein provides a good initial structure for further investigation of the architecture. Further, CAE believes 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.

CAE recommends that a valuable next step would be a prototype implementation of the four layer architecture based on at least one use case to allow engineering issues arising from this report to be examined, to allow the data model to be extended to the same level of detail as existing data models, and to validate the initial results.

1 INTRODUCTION

This document is the final report for the project entitled: *Information Warfare Simulation Architecture Development*. This report was completed by CAE Inc. (CAE) for contract #W7719-155268/001/TOR to Defence Research and Development Canada (DRDC) – Atlantic Research Centre administered by Public Services and Procurement Canada (PSPC).

1.1 Background

As described in the task Statement of Work (SOW) (Defence Research and Development Canada, 2017), under a previous task authorization an initial investigation of issues was conducted concerning the addition of an information layer to legacy computer generated forces (CGF) simulations, and a multi-national workshop on the subject was supported (Dubreuil, 2016). The workshop generated an initial architecture and a set of recommendations for moving toward a standard architecture for information warfare (Hazen, Lloyd, & Harris, The Evolution of Computer Generated Forces (CGF) Architectures to Support Information Warfare Effects, 2016).

The Royal Canadian Navy (RCN) has recently consolidated a range of existing capabilities under the banner of Information Warfare (IW) and, specifically, Maritime Information Warfare (MIW). Some of these capabilities were already being leveraged by the RCN, others (such as cyber) have proven less easy and, until recently, less critical to deploy. The efforts by the RCN to develop a concept and associated tactics, techniques and procedures (TTPs) to employ MIW follow the development and endorsement by the Five Eyes partners (Australia, Canada, New Zealand, United Kingdom and United States) of the following definition of MIW:

> "The provision, assured use and protection of information, processes, systems and networks, and the limiting, degrading and denying of that of our adversaries, to achieve operational advantage across the battlespace."

The RCN's Concept for Maritime Information Warfare (Director General Naval Force Development, 2015) notes that information has always been critical to success in warfare. The RCN recognise, however, that information has become a force multiplier as force numbers are reduced. Further, given the ubiquity of media coverage of events, the RCN must compete in a battle of narratives with an adversary. Given the scrutiny of the military, effects must be delivered with greater precision than ever before, leading to an absolute dependency on accurate and timely information. The adversary, however, often has access to the same information as the RCN thus, to achieve mission success, the right capabilities and functions must be available to the Commander.

In (Director General Naval Force Development, 2015) the RCN identified the following functional areas of activity in MIW:

- Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) comprised of:
    - Command and Control (C2);
    - Communications and Information Systems (CIS); and
    - Intelligence, Surveillance and Reconnaissance (ISR).
- Understanding and Situational Awareness of the Battlespace concerning:
    - The Tactical Picture;
    - The Common Operating Picture (COP);
    - Maritime Domain Awareness (MDA); and
    - Battlespace Management.
- Intelligence, including capabilities needing special attention to meet maritime force requirements:
    - Geospatial intelligence;
    - Signals Intelligence (SIGINT);
    - Acoustic Intelligence (ACINT); and
    - Human Intelligence (HUMINT).
- Cyber-Electromagnetic Activities (CEMA) comprised of:
    - Electronic Warfare (EW), defined according to 5 Eyes/United States (US) doctrine as:
        - Electronic Attack (EA);
        - Electronic Protection (EP); and,
        - Electronic Warfare Support (ES).
    - Cyber;
    - Defensive Cyber Operations (DCO), including Internal Defensive Measures (IDM) and Response Actions (RA);

  - Offensive Cyber Operations (OCO); and
  - Computer Network Exploitation (CNE).
- Capabilities at the Joint Level, including:
  - Information Operations; and
  - Targeting.

The MIW concept is not new, but has rarely been the subject of full scale simulation, be it for training, analysis, or in support of operations. Such a comprehensive MIW simulation capability is the objective. For example, a successful MIW training simulation will need to permit a training audience to adequately plan and execute MIW operations across all functional areas listed above, including leveraging and integrating with joint capabilities. The current work describes an architecture to support a comprehensive MIW simulation capability and uses a subset of the MIW functionality as a proof-of-concept to demonstrate the viability of such a training simulation.

1.2 Objective

The objective of this task was to implement a number of the recommendations from the workshop as part of Canada's contribution to the international effort to develop an IW simulation capability.

The first step was to develop a use case that encapsulates multiple areas of IW to frame the scope of the task. The architecture developed during the multi-national workshop was investigated and expanded, and then linked to the elements of the use case to provide a detailed example. Each step in the use case was then analysed to identify the types of activities and systems involved, and the architectural layers that they belong to. A sample data model was then created by analysing the components in the use case, and the interactions between components and the objects passed in those interactions.

Throughout this project, guidance and support was provided by the task Technical Authority (TA).

The result of this work was presented at two North Atlantic Treaty Organization (NATO) conferences: an Information Systems Technology Panel (IST) / NATO Modelling and Simulation Group (NMSG) Workshop on Cyber Effects in Campaign and Mission Simulations from 18–21 July 2017 (Hazen, Harris, & Lamoureux, Extending Computer Generated Forces (CGF) Architectures to Support Information Warfare and Cyber Effects, 2017) and a NATO MSG Symposium on "M&S Technologies and Standards for Enabling Alliance Interoperability and Pervasive M&S Applications" from 19–20 October 2017 (Hazen, Harris, & Lamoureux, Use Case Analysis of the Information Warfare Engagement Model Architecture, 2017).

1.3 Document Organization

The structure of this document is as follows:

- Section 1: Introduction – describes the background and objective of the work conducted during this project;
- Section 2: References – provides a list of references used in this report;
- Section 3: Use Case – describes the use case used to motivate and drive the development of the Information Warfare Simulation Architecture (IWSA);
- Section 4: Architecture Functionality – describes the layers, components and effects contained within the IWSA using the use case to provide specific examples;
- Section 5: Architecture Layer Interfaces – describes the various considerations to be applied in defining interfaces within and across the various layers of the architecture;
- Section 6: Data Model – describes the interactions and objects that apply at simulation initialization and run-time for the use case, and proposes an example Information Warfare Simulation Data Model (IWSDM) to represent those interactions and objects; and
- Section 7: Discussion and Recommendations – concludes with a discussion and presents recommendations arising from this project.

2 REFERENCES

Bernier, M. (2013). *Military Activities and Cyber Effects (MACE) Taxonomy.* Defence Research and Development Canada Centre for Operational Research and Analysis.

Boyd, J. R. (1995). *The Essence of Winning and Losing.* Retrieved July 5, 2017, from https://web.archive.org/web/20110324054054/http://www.danford.net/boyd/essence.htm

Bratman, M. E. (1987). *Intention, Plans, and Practical Reason.* CSLI Publications.

Cockburn, A. (2000). *Writing Effective Use Cases.* Addison-Wesley.

Defence Research and Development Canada. (2017). *TA-12 – Information Warfare Simulation Architecture Development Statement of Work.*

Director General Naval Force Development. (2015). *Concept for Maritime Information Warfare.* Royal Canadian Navy.

Dubreuil, A. (2016). *Human Factors Research and Modelling: Task 4 Investigation of Computer-Generated Forces Modelling of Information Layer Effects.* Defence Research and Development Canada.

Fowler, M. (1999). *UML Distilled: A Brief Guide to the Standard Object Modeling Language* (2nd ed.). Addison-Wesley.

Hazen, M. G., Harris, E., & Lamoureux, T. (2017). Extending Computer Generated Forces (CGF) Architectures to Support Information Warfare and Cyber Effects. *MSG-151 Workshop on Cyber Effects in Campaign and Mission Simulations.* Portsmouth, UK.

Hazen, M. G., Harris, E., & Lamoureux, T. (2017). Use Case Analysis of the Information Warfare Engagement Model Architecture. *MSG-149 Symposium on M&S Technologies and Standards for Enabling Alliance Interoperability and Pervasive M&S Applications.* Lisbon, Portugal.

Hazen, M. G., Lloyd, J. P., & Harris, E. (2016). The Evolution of Computer Generated Forces (CGF) Architectures to Support Information Warfare Effects. *MSG-143 Symposium on Ready for the Predictable, Prepared for the Unexpected - M&S for Collective Defence in Hybrid Environments and Hybrid Conflicts.* Bucharest, Romania.

IEEE. (1995). *IEEE Std 1278.1-1995: IEEE Standard for Distributed Interactive Simulation – Application Protocols.* IEEE.

IEEE. (1998). *IEEE Std 1278.1a-1998: IEEE Standard for Distributed Interactive Simulation – Application Protocols.* IEEE.

IEEE. (2010). *IEEE Std 1516.1-2010: IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Federate Interface Specification.* IEEE.

IEEE. (2010). *IEEE Std 1516.2-2010: IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Object Model Template (OMT) Specification.* IEEE.

IEEE. (2012). *IEEE Std 1278.1-2012: IEEE Standard for Distributed Interactive Simulation – Application Protocols.* IEEE.

Internet Engineering Task Force. (1989). *Requirements for Internet Hosts -- Communication Layers.* Internet Engineering Task Force. Retrieved July 4, 2017, from https://tools.ietf.org/rfc/rfc1122.txt

ISO/IEC. (1994). *ISO/IEC 7498-1: Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model* (2nd ed.).

MIP. (2012). *The Joint C3 Information Exchange Data Model (JC3IEDM Main).* Multilateral Interoperability Programme.

MIP. (2017). *MIP Information Model (MIM) – Version 4.1.* Multilateral Interoperability Programme.

Musman, S., Temin, A., Tanner, M., Fox, D., & Pridmore, B. (2010). Evaluating the Impact of Cyber Attacks on Missions. In E. Armistead, & E. Cowan (Ed.), *Proceedings of the 5th International Conference on Information Warfare and Security*, (pp. 446-456). Dayton, Ohio.

Osinga, F. (2005). *Science, Strategy and War The Strategic Theory of John Boyd.* Eburon Academic Publishers. Retrieved July 5, 2017, from http://www.projectwhitehorse.com/pdfs/ScienceStrategyWar_Osinga.pdf

Pitch Technologies. (2014). *The HLA Tutorial.* Retrieved July 05, 2017, from http://www.pitchtechnologies.com/wp-content/uploads/2014/04/TheHLAtutorial.pdf

Rao, A. S., & Georgeff, M. P. (1991). Modelling Rational Agents within a BDI-Architecture. *Proceedings of the 2nd International Conference on Principles of Knowledge Representation and Reasoning* (pp. 473-484). Cambridge, MA, USA: Morgan Kaufmann.

Selvestrel, M., Harris, E., & Ibal, G. (2004). SM Agent Technology For Human Operator Modelling. *Proceedings of the SimTecT 2004 Simulation Conference.* Canberra, ACT, Australia. Retrieved July 5, 2017, from http://www.simulationaustralasia.com/files/upload/pdf/research/094-selvestrel-2004.pdf

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

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

SISO. (2015). *SISO-STD-007-2008: Standard for Military Scenario Definition Language (MSDL).* SISO.

SISO. (2017). *C2SIM PDG/PSG - Command And Control Systems - Simulation Systems Interoperation*. Retrieved August 3, 2017, from Simulation Interoperabilty Standards Organization: https://www.sisostds.org/StandardsActivities/DevelopmentGroups/C2SIMPDGPSG-CommandandControlSystems.aspx

Tanenbaum, A. S. (1981). *Computer Networks.* Prentice/Hall International.

Tidhar, G., Heinze, C., Goss, S., Murray, G., Appla, D., & Lloyd, I. (1999). Using Intelligent Agents in Military Simulation or "Using Agents Intelligently". *Proceedings of the Eleventh Conference on Innovative Applications of Artificial Intelligence* (pp. 829-837). Orlando, FL, UYSA: The AAAI Press.

Wikipedia. (2017, June 17). *Internet protocol suite*. Retrieved July 4, 2017, from Wikipedia: https://en.wikipedia.org/wiki/Internet_protocol_suite

Wikipedia. (2017, July 3). *OSI model*. Retrieved July 4, 2017, from Wikipedia: https://en.wikipedia.org/wiki/OSI_model

Wikipedia. (2017, July 4). *Solution stack*. Retrieved July 4, 2017, from Wikipedia: https://en.wikipedia.org/wiki/Solution_stack

3 USE CASE

NOTE: The information warfare capabilities represented in this use case are not representative of current RCN doctrine and have been chosen in order to investigate particular aspects of the architecture.

This section contains the use case used to provide a context for exploring the further development of the IWSA.

The use case describes an IW simulation used to support the training of Maritime Staff Officers conducting IW in a Maritime Interdiction Operation (MIO) against suspected human smugglers.

At an operational level, the use case is for a Task Group (TG) to conduct a Maritime Interdiction Operation (MIO) against suspected human smugglers. Naval staff officers play the role of the Commander of the Task Group (CTG) staff following existing processes and interacting with standard systems. Behind this, the remainder of the TG, including communications systems and the IW implementing resources, and the adversary are all modelled by a CGF. The CGF interprets the plans received from the CTG staff, executes the plan against the adversary, and models the adversary's response and the success or failure of the plan.

For the purposes of this use case, the CGF is a future idealised CGF in comparison to the CGFs (or simulation federations) of today that would typically require multiple systems, training staff, CGF pucksters and exercise white force personnel to implement this use case. We consider that this future CGF may consist of multiple, distributed parts; for the purposes of this report we nonetheless label the resulting system as a CGF.

The use case has been decomposed into two parts described below: Present Information Warfare Simulation and Present Offensive Cyber Operation (OCO) Simulation. The Present OCO Simulation use case represents a sub-element of the Present IW Simulation use case that represents an offensive cyber operation in more detail. The Present IW Simulation use case is very broad and therefore provides the framework for our discussion, while in this report, we concentrate on the details of the Present OCO Simulation use case.

Figure 3-1 shows the human and CGF actors involved in the use case. The CTG Staff are the trainee Maritime Staff Officers, while the other elements of the TG and the Adversary are simulated by the CGF. The colour of the actors in Figure 3-1 denotes the affiliation within the scenario (black indicates neutral affiliation).

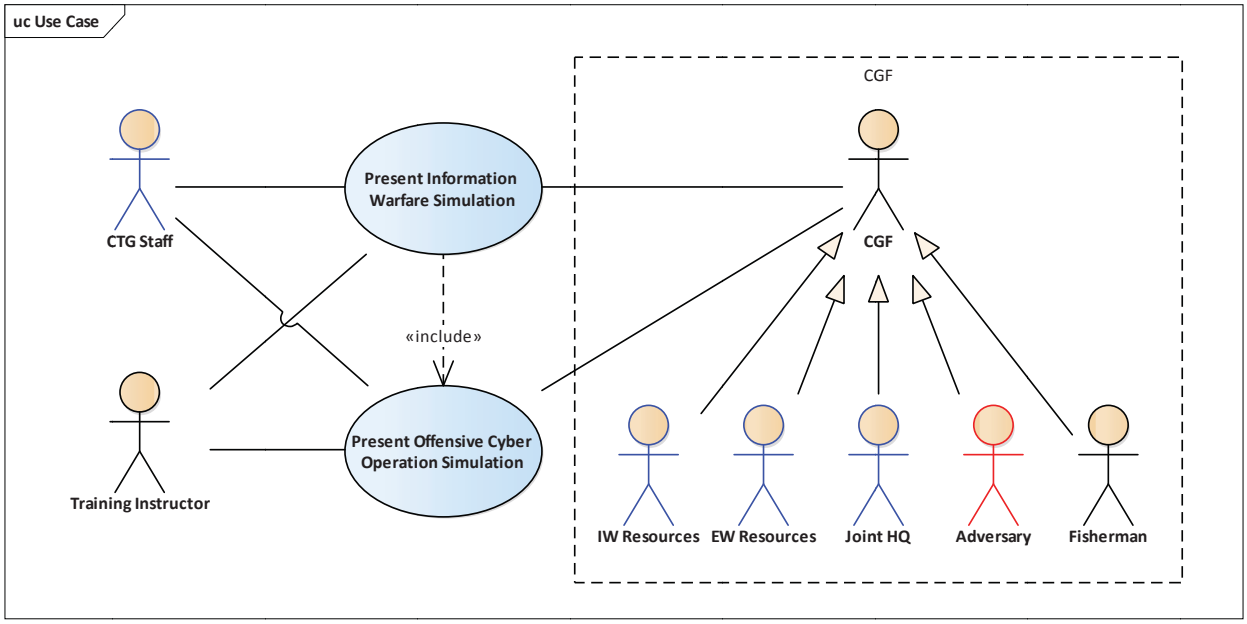

Figure 3-1: Human and CGF Actors Involved in the Use Case

3.1 Use Case Template

The use cases are presented in two forms: the first is as a table that conforms with Cockburn's fully dressed form for use cases (Cockburn, 2000); the second is as a sequence of steps as suggested by Fowler (Fowler, 1999).

Cockburn's fully dressed use case form uses thirteen different structural elements to result in a comprehensive use case. These elements are described in Table 3-1.

Table 3-1: Elements of Cockburn's Fully Dressed Use Case Form

Element	Description
Title	A succinct statement of the goal to be achieved by the primary actor. The title should use an active verb to describe the goal.
Primary Actor	The system stakeholder with the goal that the use case addresses. The person who requires the system to perform some function. There may be other stakeholders.
Goal in Context	What does the system have to achieve, under what conditions and within what performance parameters?
Scope	What is the size of the system being described? What elements are deliberately inside the scope and deliberately outside the scope?
Level	With respect to the system itself, does the use case provide a summary level

Element	Description
	of detail, a user level of detail, or a sub-function level of detail?
Stakeholders and Interests	People with a vested interest in the system, even if they never interact with the system. Stakeholders should be described according to the specific nature of their relationship with the system, whether they receive some output, are responsible for its upkeep, need to recruit and train operators, or finance the purchase of the system.
Precondition	What condition has to be true, or completed or otherwise satisfied before the activity described in the use case can be begun?
Minimal Guarantees	The minimal set of functions or outputs the system will deliver to the stakeholders, in particular if the primary actor's goal cannot be achieved.
Success Guarantees	A description of the state or output that the primary actor wants to achieve.
Trigger	The specific event that will invoke the system and/or functions described in the use case.
Main Success Scenario	A step-by-step description of how the use case would be satisfied by a system if nothing went wrong or 'off' the expected trajectory. Begins with the trigger.
Extensions	Descriptions of possible variations from the main success scenario.
Technology and Data Variations List	From a technical perspective, identifying different methods for inputting data or actions into the system and outputting results from the system, and different data formats that may be required to develop an implementation of the use case.

Cockburn also describes a casual use case form. The casual form shares the Title, Primary Actor, Scope and Level, but adds a **Story**, which is a plain English description of the events and activities that occur (i.e., inputs relevant to the use case), the actions of the primary actor, what arises from these actions, and the impacts (i.e., outputs) on the external world. The use cases described in this report follow the fully dressed form and add the Story element.

Fowler suggests (Fowler, 1999) using a sequence of numbered steps for the primary (main success) scenario with alternatives (extensions) presented as variations on that sequence. In this report, for detailed use cases we also provide a description of the Story as a sequence of steps.

3.2 Present Information Warfare Simulation

Table 3-2 contains a description of the Present Information Warfare Simulation use case according to Cockburn's fully dressed form.

Table 3-2: Present Information Warfare Simulation Use Case

Field	Description
Title	Present Information Warfare Simulation

Field	Description
Primary Actor	CTG Staff
Goal in Context	CTG Staff plan an MIO operation against human smugglers which take advantage of IW capabilities. CTG Staff must enter this plan into their C2 system (can be via orders to subordinate units) that results in simulated execution of this plan by a CGF and will provoke simulated responses from the CGF. The simulated responses must be 'sensed' and presented to the CTG Staff in some way. Because this application is for a training simulation, performance metrics are also drawn from the simulation for after-action review with the CTG Staff.
Scope	The MIO operation plan, a set of IW capabilities that may be used, the means by which the plan is entered into the CGF, the simulation of the IW capabilities and effects, the simulated response from the CGF (including unintended effects), the presentation of this response to the training audience.
Level	Summary, User Goals, Sub-Functions

Stakeholders and Interests	CTG Staff who require an ability to plan and communicate MIO operation using IW capabilities that 'shapes' the information and decision space of the task group and adversary, monitor effects, formulate response if necessary.
	Training staff who will use the CGF to support achieving their training goals, and generate metrics allowing them to assess training progress.
	Support staff who need to operate (and validate) the CGF to support the training functions.
	Additional Stakeholder interests include the simulation of IW capabilities:
	• C4ISR: C2; CIS; ISR
	• Understanding and Situational Awareness of the Battlespace:
	  ○ Tactical Picture
	  ○ COP
	  ○ Battlespace Management
	• Intelligence: Geospatial; SIGINT; ACINT; HUMINT
	• Cyber-Electromagnetic Activities:
	  ○ EW: EA; EP; ES
	  ○ Cyber: DCO (IDM and RA); OCO and CNE
	• Capabilities at the Joint Level:
	  ○ Information Operations
	  ○ Targeting

Precondition	The means exist to execute an IW task. Sufficient information exists and is accessible to the CTG Staff to allow them to plan using an IW task. The means exist to determine the effects of the IW task execution using real and/or simulated equipment, including a CGF. Training instructors have the means to collect data to evaluate and critique performance.
Minimal Guarantees	That the IW plan is accepted by the CGF and the CTG Staff receive feedback concerning its success or failure that is clearly responsive to the nature of the input

Field	Description
	and the situational context.
Success Guarantees	Feedback to indicate how the target (CGF adversary) is responding to IW inputs. Training instructors are able to provide specific and timely feedback to CTG Staff concerning their performance in the scenario.
Trigger	CTG Staff wish to incorporate an IW element to a mission plan.
Main Success Scenario	CTG Staff plan an MIO operation that includes IW operations and input the plan into their C2 system whereby it is executed by simulated subordinate formations in a CGF. CGF units react to the IW tasks with changed behaviour. Data on the effect of the MIO operation is generated and relayed to the CTG Staff so they receive feedback on the success or failure of their MIO operation. Performance data is collected from the CGF to be subject to post-hoc analysis by training instructors.
Extensions	The IW plan fails. Subordinate Units are disabled or otherwise removed from the IW chain of actors. The C2 capabilities of the TG are reduced or destroyed.
Technology and Data Variations List	None.
Story	CTG Staff are developing a plan to carry out an MIO to combat human smugglers. The plan is comprehensive and includes manoeuvre, rules of engagement (ROE) to include kinetic effects, vessels and persons of interest, and information warfare. CTG has limited forces at his disposal and wishes to maximize the chances of interdicting the vessel of interest (VOI). To do this an IW plan is developed to influence and deceive the adversary and reduce their perceived decision space and options by convincing them that their intelligence is both credible and verifiable and indicates that the force disposition will be toward certain areas of the operation (op) area. This will convince the adversary to avoid the TG by taking a different route, which the TG will predict and interdict. Further, the IW plan will also promulgate falsehoods about the sensor capability and range of the TG, fooling the adversary into moving when chances of detection are presumed to be small but are, in fact, at their highest. The TG will also attempt to identify and exploit electronic devices being used by the traffickers, both through communications interception as well as accessing data on the devices. Finally, the CTG IW plan will attempt to influence the populace to believe that the human traffickers are evil and seek to exploit and hurt those wishing to travel for a better life. This will help to ensure that the boarding parties are not met with hostility and are supported by those being trafficked. The CTG Staff must pass this plan to the ships in their TG. Each ship has an embedded IW team with particular capabilities to execute an IW operation. Along with these capabilities is the ability to carry out a variety of intelligence gathering activities to determine if and how well the IW operation has an effect on the target. Through HUMINT, traditional passive surveillance, monitoring of radio and television (TV), webcams and social media, the ships are able to determine the progress of the IW operation and determine how it should be adapted and how the more traditional elements of the plan (manoeuvre, kinetic, etc.) need to change to

Field	Description
	match the emerging situation. The CTG Staff receive this feedback from the ships and coordinate a reaction that is optimized across the force, rather than individually for the ships. At the conclusion of the simulation the training instructors are able to use data collected from the exercise to provide accurate and timely feedback to the CTG Staff in order that they may learn and improve their performance.

Table 3-3 lists operational systems that are present and used in the Present Information Warfare Simulation use case, categorised by the type of the system and the affiliation of the system.

Table 3-3: Operational Systems Employed in Present Information Warfare Simulation Use Case

Affiliation	System Type	Operational System
Friendly	Human	• CTG Staff • IW Resources staff • Boarding parties
	Computer / Hardware	• CTG Staff computers • CTG Staff network (servers, routers) • IW Resources computers • IW Resources network (servers, routers)
	Computer / Applications	• CTG Staff e-mail system • CTG Staff chat system • CTG Staff C2 system (including COP, planning) • IW Resources e-mail system • IW Resources chat system • Web Services client
	Computer / Data	• CTG Staff e-mail content • CTG Staff chat content • CTG Staff C2 data (COP, etc.) • IW Resources e-mail content • IW Resources chat content • Military Message content • Web Services content (received & displayed locally)
	Communications	• Marine Radio • Satellite Communications (SATCOM) • Automatic Identification System (AIS)

Affiliation	System Type	Operational System
		• Cell phones • Military Message system • CTG Staff Local Area Network (LAN) • IW Resources LAN • TG Wide Area Network (WAN) • National or Coalition Network (WAN) • Commercial Internet access
	Counter-countermeasures	• Electronic Protection • Defensive Cyber Measures
	Sensors	• Navigation radar • Tracking radar • Acoustic • EOIR detect and track
	Sensors / IW	• Visual • HUMINT
	Sensors / EW	• Electronic Warfare Support • Communications Intelligence (COMINT) • Electronic Intelligence (ELINT) • SIGINT
	Sensors / Cyber	• Digital Defences at network gateways (intrusion detection systems (IDS), virus scanners, etc.) • User reporting procedures for system irregularities • Social media tracking
	Effectors / Weapons	• Kinetic weapons (main gun, .50 cal mg, land attack missiles) • Small arms (boarding parties)
	Effectors / Electronic	• Electronic Attack (jamming, pulse)
	Effectors / Cyber	• Cyber Attack systems
	Effectors / Influence	• Propaganda
	Platforms	• TG ships • Aircraft • Autonomous vehicles
Hostile	Human	• Adversary (human smugglers)
	Computer / Hardware	• Laptops • Mobile devices
	Computer / Applications	• Cell phone e-mail client

Affiliation	System Type	Operational System
		• Cell phone web browser
	Computer / Data	• E-mail content • Short Message Service (SMS) messages • Web Services content
	Communications	• Marine Radio • AIS • Cell phones • Wi-Fi network
	Sensors	• Navigation radar
	Sensors / Human	• Visual (binoculars)
	Sensors / Cyber	• Digital Defences at network gateways (commercial off-the-shelf (COTS) anti-virus (AV), threat detection)
	Effectors / Weapons	• Small arms • Shoulder launched missiles
	Effectors / Influence	• Propaganda
	Platforms	• VOI • Ashore sites
Neutral	Human	• Populace • Humans smuggled
	Computer / Hardware	• Mobile devices • Webcams • Commercial Internet Service Provider (ISP) systems
	Computer / Applications	• E-mail systems • Social media systems and clients • Commercial Web Services
	Computer / Data	• E-mail content • Social media content • Web Service content
	Communications	• Cell phones • Cell phone network • Internet • Marine Radio • Television • AIS • Physical news media (newspapers, leaflets)

Affiliation	System Type	Operational System
	Sensors	• Navigation radar
	Sensors / Human	• Visual
	Platforms	• Shipping • Fishing boats • Pleasure craft • Ashore sites
Training	Human	• Instructor

3.3 Present Offensive Cyber Operation Simulation

Table 3-4 contains a description of the Present Offensive Cyber Operation Simulation use case according to Cockburn's fully dressed form. The categorisation of specific cyber effects into interruption, modification, degradation, fabrication, interception and unauthorised use is due to Musman et al. (Musman, Temin, Tanner, Fox, & Pridmore, 2010) and is as discussed by Bernier (Bernier, 2013).

Table 3-4: Present Offensive Cyber Operation Simulation Use Case

Field	Description
Title	Present Offensive Cyber Operation Simulation
Primary Actor	CTG Staff
Goal in Context	CTG Staff plan an IW operation to support MIO against human smugglers. The IW operation will include OCO and CNE. CTG Staff must enter this OCO plan into a system (can be via orders to subordinate units) that results in simulated execution of this plan by a CGF and will provoke a simulated response from the CGF adversary. This simulated response must be 'sensed' and presented to the CTG Staff in some way. Because this application is for a training simulation, performance metrics are also drawn from the simulation for after-action review with the CTG Staff.
Scope	The IW plan, the means by which the plan is entered into the simulation, the simulation of the IW effects, the simulated response from the CGF adversary (including unintended effects), the presentation of this response to the training audience, the collection of performance data for post-hoc analysis.
Level	Summary, User Goals, Sub-Functions
Stakeholders and Interests	• CTG Staff who require: intelligence on the adversary to permit them to select and deploy a suitable OCO approach; the ability to plan and communicate OCO tasks to subordinate units, monitor effects, and formulate response if necessary. • Training staff who will use the CGF to support achieving their training goals, and generate metrics allowing them to assess training progress.

Field	Description
	• Support staff who need to operate (and validate) the CGF to support the training functions.
Precondition	• CTG Staff have the means to enter their OCO plan into the CGF, either directly or via their subordinate units. • The CGF has the capacity to represent the different types of OCO of interest (phishing, spear-phishing, SQL Injection Attack, XSS, DOS Attack, Session Hijacking/Man-In-The-Middle Attack, Credential Reuse, Malware, CNE). • CTG staff have the means to determine the effect of their OCO. • Training instructors have the means to collect data to evaluate and critique performance.
Minimal Guarantees	That the OCO plan can be entered into the CGF and the CTG Staff receive some feedback concerning the effect created by the OCO.

Success Guarantees	• The CTG Staff are able to communicate the plan to simulated subordinate units (CGF).
	• The plan consists of the desired effect and associated tasks/timings/schedule/milestones.
	• CTG Staff receive feedback on the plan, questions/requests for clarification from the simulated subordinate units (CGF).
	• CTG Staff receive feedback on the execution of the plan.
	• CTG Staff receive feedback on the success or failure of the plan:
	  ○ Feedback to CTG Staff would most likely be via CHAT.
	  ○ Feedback would indicate that access to adversary network(s) has been established, that malware has been installed, and that the specific effect (see below) has been achieved through active manipulation of the adversary's assets. By assuming active manipulation, the feedback to CTG Staff would come from the individual or team associated with the subordinate tactical unit. Additionally, if there has been malware installed, this can send a signal back to the subordinate tactical unit, or harvest data and save it to a server to retrieval by the subordinate tactical unit. Feedback concerning active manipulation or automated interventions would/could apply in any of the cyber effects described below.
	  ○ Feedback indicating that the OCO has not been successful would come from the tactical unit and indicate that they have not been able to access the adversary network(s), or that they had received no confirmation that the malware has been installed, or that they are not receiving data to indicate that the OCO has been successful, or via Comms EW intercepting radio, cell phone or social media traffic from the adversary.
	  ○ As noted elsewhere in this use case, detection of a CGF adversary cyber attack, thus requiring DCO, would be indicated to CTG Staff by the subordinate unit with cyber defence capabilities. These units will likely be searching for unauthorised packets at network gateways.
	  ○ Specific cyber impacts/effects on the CGF adversary via attack vectors are:
	  ▪ Interruption of CGF adversary asset (unusable, unavailable or lost for specific period of time); feedback to CTG Staff via chat that a CGF

Field	Description
	adversary has clicked on the link, that malware has been installed, that data is being harvested. ▪ Modification of CGF adversary asset (of information, data, protocol or software). ▪ Degradation of CGF adversary asset (of performance). ▪ Fabrication (information is inserted into CGF adversary system). ▪ Interception (attacker causes or takes advantage of information leaked from CGF adversary system). ▪ Unauthorized Use (attacker uses system resources for his own purpose). • The actions of the CGF adversary change as a response to the OCO resulting in a greater probability of mission success. Ideally feedback to this effect will be communicated to CTG Staff. • Specific Outcomes (these assume that CGF adversary does not have the ability to engage in OCO themselves which, if they do, would likely form part of the response if the CTG OCO is detected): ○ Phishing: low probability of success: CGF adversary clicks on a link in generic, broadly targeted email allowing the installation of malware on CGF adversary's device (probably cell-phone, possibly laptop); Failure mode is that CGF adversary's vigilance increases concerning OCO and they may be able to reverse-engineer information in the email to determine the origin and engage in defensive cyber operations, they complain on social media and/or to colleagues via cell phone. ○ Spear-Phishing: high probability of success: CGF adversary clicks on interesting link in specifically targeted email allowing the installation of malware on CGF adversary's device; Failure mode is that CGF adversary's vigilance increases concerning OCO and they may be able to reverse-engineer information in the email to determine origin and engage in defensive cyber operations, they complain on social media and/or to colleagues via cell phone. ○ SQL Injection Attack: medium probability of success: CGF adversary are unlikely to have databases but wireless service providers probably do; depends how much SIGINT the TG has about the infrastructure; if successful, much data will be held about names, numbers, frequency of calls, timing of calls, etc. delivered directly or via CNE activities; CGF adversary can be fed misleading information; Failure mode is that CGF adversary vigilance increases with additional security being layered on top of existing security and procedures being enacted to discover sources of HUMINT, may direct attacker to duplicitous data, they complain on social media and/or to colleagues via cell phone. ○ XSS: Medium probability of success: similar to SQL Inject, but embedded on a website, blog or forum that CGF adversary might frequent. Same successful outcomes as SQL Inject; Same failure outcomes as SQL Inject. ○ DOS Attack: high probability of success: overload the CGF adversary's networks and eliminate their ability to communicate, sense, target, etc. Basically disrupt their C4ISR. CGF adversary becomes paralysed until they

Field	Description
	can remedy the situation, which would likely be as long as CTG choose to persist in the DOS Attack; Failure mode is that CGF adversary realise they are being target and find alternative means to carry out C4ISR, they complain on social media and/or to colleagues via cell phone. ○ Session Hijack/Man-In-The-Middle Attack: Probability of success dependent upon SQL Inject or XSS, but medium if they succeed: Gather credentials and other information that permit CNE data mining activities; Failure mode is that CGF vigilance increases concerning OCO and they may be able to reverse engineer to determine origin and engage in defensive cyber operations, they complain on social media and/or to colleagues via cell phone. ○ Credential reuse: unlikely to be used. ○ Malware: high probability of success once installed: permit TG to engage in data harvesting and CNE activities; Failure mode is that CGF adversary will examine their networks and find other evidence of compromise, determine origin and engage in defensive cyber operations, they complain on social media and/or to colleagues via cell phone. ○ CNE: high probability of success once a vulnerability is found and exploited; permit TG to engage in data harvesting, send commands to automated systems, inject errors into targeting data, actively destroy GPS navigation systems by sending malicious commands; Failure mode is the CGF discover they are being attacked and engage in defensive cyber operations, they complain on social media and/or to colleagues via cell phone. • Training instructors are able to provide specific and timely feedback to CTG staff concerning their performance in the scenario.
Trigger	CTG staff wish to incorporate an OCO element to a mission plan.
Main Success Scenario	• CTG Staff request the allocation of IW Resources owned by Joint HQ as CGF subordinate unit, and request is granted. • CTG Staff enter OCO plan into the communications system that transmits it to the CGF subordinate unit. • CTG Staff receive acknowledgement from CGF subordinate unit that plan was received successfully and is accepted, questioned, rejected. • OCO plan is executed by the CGF subordinate unit. • OCO has an effect on the actions of the CGF adversary. • Effects on CGF adversary are detected by the CGF subordinate unit. • Effects on CGF adversary are communicated to CTG Staff. • CTG Staff are able to alter ongoing execution of OCO, or discontinue. • Performance data is collected from the CGF to be subject to post-hoc analysis by training instructors.
Extensions	• The CGF subordinate unit(s) have questions about the OCO plan. • The CGF subordinate unit(s) reject the OCO plan. • The CGF subordinate unit(s) apply their own opinions and cognitive biases in

Field	Description
	executing the OCO plan. • The OCO fails to result in an effect on the CGF adversary. • The CGF adversary accurately deduce they are the target of an OCO and deliberately feed misleading information back to CTG Staff. • The CGF adversary conduct their own OCO against the TG. • Subordinate Units are disabled or otherwise removed from the OCO chain of actors. • The C2 capabilities of the TG are reduced or destroyed.
Technology and Data Variations List	None.
Story	CTG Staff plan an MIO to combat human smuggling. Intelligence indicates that there are multiple possible routes the human smugglers may take and that at least one of the smuggled humans is a person of interest to the coalition. The TG has insufficient units to cover all routes. As part of this operation they wish to make use of their OCO and CNE capabilities to limit the probable route to ones where the TG has a high probability of intercept and success. Candidate OCO and CNE methods and desired outcomes considered include: • Access the GPS receiver software in the mobile phones of the human smugglers. Alter the software to apply an offset in order to delay the human smugglers while they manually correct course, while also reducing the likely area and routes that the human smugglers will likely use, thus increasing the chances of interdicting them. • Access weather feeds used by the human smugglers and alter them to indicate that conditions (e.g., wind direction and strength, currents, sea state) are not favourable to embark. This delay would provide additional opportunity to work with ground forces and local security forces to interdict the human smugglers while still ashore. • Create a social media feed providing misleading statements concerning operations of TG ships. Human smugglers are misled into believing ships are operating in different locations or not concerning with human smuggling. Misdirection results in human smugglers sailing directly into MIO. • Post geo-tagged pictures of TG ships indicating incorrect location. Position geo-tags such that human smugglers choose to follow a different route which is advantageous to the TG. • Access AIS transponder of human smuggler ship and set to ‘transmit’. • Access navigation system of ship and alter position, course and speed information to direct human smugglers to TG ships. • Appear as fellow human smuggler via email and/or SMS and arrange meeting time and location. Subsequently disable human smugglers’ cell phones. • Access the information databases used by the human smugglers (for instance, contacts, financial records, code words, location history on mobile phone) and insert false information that will direct the human smugglers to feed information to, or actively collaborate with, TG resources such that the TG increases the

Field	Description
	likelihood of a successful operation. In possession of sufficient HUMINT and SIGINT to permit them to select the appropriate OCO and CNE approaches, the CTG Staff request the allocation of IW Resources owned by Joint HQ as subordinate units. When granted, CTG Staff communicate the plan to the CGF subordinate units with the appropriate OCO and CNE capabilities. Taking into account their own opinions and cognitive biases, the CGF subordinate units (IW Resources and EW Resources) execute the plans and communicate the results to the CTG Staff. The CTG Staff fold these results into ongoing planning to increase the probability of success of the MIO mission. The CTG Staff must consider, however, that the adversary may realise they are under cyber attack and have, themselves, responded with deceptive information and may be gathering intelligence against the TG. At the conclusion of the simulation the training instructors are able to use data collected from the exercise to provide accurate and timely feedback to the CTG Staff in order that they may learn and improve their performance.

The specific steps involved in the basic scenario of the Present OCO Simulation use case corresponding to the Main Success Scenario and the first and third of the Extensions are:

1. CTG Staff prepares an OCO plan consisting of the following steps:
    a. Use social media to encourage Adversary to choose a route that the TG can intercept.
    b. Infiltrate Adversary cell phones and/or laptops to confirm location in port; e-mail addresses have been supplied by HUMINT.
    c. Monitor Adversary cell phones (calls, messages, etc.) to determine their plans (i.e., when human smuggling will occur).
    d. Monitor Adversary cell phones to determine when the Adversary leaves port.
    e. Route TG to intercept Adversary.
    f. Detect and track Adversary with radar and EO/IR when in range.
    g. Monitor Adversary cell phones and marine radio to help determine if TG is detected.
    h. Disable Adversary cell phones and marine radio just prior to interception.
2. CTG Staff requests allocation of IW Resources from Joint HQ staff as a Subordinate Unit via e-mail.
3. Joint HQ allocates IW Resources to CTG Staff via e-mail, changing the active organizational structure involving IW Resources.

4. CTG Staff sends the OCO plan to Subordinate Units (IW Resources and EW Resources) via e-mail.

5. IW Resources review the OCO plan, applying their own opinions and cognitive biases to the interpretation.

6. 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.

7. 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.

8. IW Resources decide to use Facebook, Twitter and Instagram, using different aliases, and to try spear-phishing based on HUMINT.

9. IW Resources post several messages to Facebook and Twitter using different aliases indicating the TG is in a particular area (that it is not).

10. 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).

11. Adversary sees the messages and pictures and, taking their own opinions and cognitive biases into account, decides to stay away from the indicated area.

12. IW Resources prepare and send spear-phishing e-mail directed at the Adversary, and report to CTG Staff that e-mail has been sent.

13. 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 Website #1 containing malware.

14. Malware installs on the Adversary's cell phone, then connects to Website #2 and reports Adversary's position; Adversary's anti-virus software does not detect the presence or actions of the Malware.

15. IW Resources check Website #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.

16. Adversary uses cell phone to plan human smuggling operation; Malware copies message data sent and received (SMS, e-mail, Signal) and voice recordings to Website #2.

17. IW Resources monitor Website #2 and reports plans of the Adversary to CTG Staff via e-mail.

18. Adversary departs port on a human smuggling operation; Malware connects to Website #2 and reports Adversary's position.

19. IW Resources monitor Website #2 and report departure of the Adversary to CTG Staff via e-mail.

20. CTG Staff orders TG to sail to intercept Adversary.

21. IW Resources command Malware to disable Adversary cell phone; Malware disables Adversary cell phone.

22. Colleagues of Adversary attempt, but are unable, to call Adversary via cell phone.

23. EW Resources monitor marine radio (COMINT) and hear a local fisherman discussing the TG; Adversary also hears and enters discussion.

24. Adversary changes course based on the discussion.

25. EW Resources track Adversary using EW interception and direction finding (ELINT) of marine radio discussion.

26. EW Resources jam marine radio of Adversary.

27. When in detection range, TG detect then track Adversary by radar then EO/IR then visual.

28. TG intercepts Adversary and the training scenario concludes.

29. Training Instructor analyses data recorded during the scenario and provides after-action review feedback to the trainee Maritime Staff Officers.

While valid extensions, the second and fourth Extensions in Table 3-4 do not add new systems or interactions between systems and so are not considered here. The last four Extensions are likely to add new systems or interactions between systems and so may be worth exploring in future.

This scenario includes elements that encompass data networks, transmission information content and cognitive responses to the information. Data networks include the cell phone network, internet, TG-wide network, and local area networks (LANs) on each of the TG units. Information content includes the interception and copying of cell phone messages, spear-phishing e-mail, the storage and retrieval of data on websites, and posting of messages and pictures to social media. The cognitive responses include reacting to (enabling) the spear-phishing attack e-mail, and making decisions influenced by postings to social media.

Table 3-5 lists the operational systems in the Present OCO Simulation use case, categorised by the type of the system and the affiliation of the system. The systems shown in *italics* are not directly referenced in the steps of the basic scenario above but are present and may be used in an extension in which the Adversary conducts a reciprocal OCO attack on the TG.

Table 3-5: Operational Systems Employed in Present OCO Simulation Use Case

Affiliation	System Type	Operational System
Friendly	Human	• CTG Staff • IW Resources staff • EW Resources staff • Joint HQ staff
	Computer / Hardware	• CTG Staff computers • CTG Staff network (servers, routers) • IW Resources computers • IW Resources network (servers, routers) • EW Resources computers • EW Resources network (servers, routers) • Joint HQ computers • Joint HQ network (servers, routers)
	Computers / Applications	• CTG Staff e-mail system • CTG Staff chat system • IW Resources e-mail system • IW Resources chat system • IW Resources Facebook app • IW Resources Twitter app • IW Resources Instagram app • Website #1 containing Malware • Website #2 contacted by Malware • EW Resources e-mail system • EW Resources chat system • Joint HQ e-mail system
	Computers / Data	• CTG Staff e-mail content • CTG Staff chat content (saved) • IW Resources e-mail content • IW Resources chat content (saved) • Facebook content • Twitter content • Instagram content • EW Resources e-mail content • EW Resources chat content (saved) • Joint HQ e-mail content
	Communications	• CTG Staff LAN

Affiliation	System Type	Operational System
		• IW Resources LAN • EW Resources LAN • TG WAN • Joint HQ LAN • Commercial Internet access • IW Resources cell phones • Marine Radio equipment • *SATCOM* • *AIS*
	Sensors	• *Navigation radar* • Tracking radar • EOIR detect and track
	Sensors / IW	• Visual • *HUMINT*
	Sensors / EW	• COMINT sensor • ELINT sensor • *SIGINT sensor*
	Sensors / Cyber	• *Digital Defences at network gateways (intrusion detection systems, virus scanners, etc.)* • *User reporting procedures for system irregularities* • *Social media tracking*
	Effectors / Cyber	• Malware
	Effectors / EW	• Jammer
	Platforms	TG ships: • CTG Staff ship • IW Resources ship • EW Resources ship
Hostile	Human	• Adversary • Adversary colleagues
	Computer / Hardware	• Mobile devices
	Computer / Applications	• Cell phone e-mail client • Cell phone web browser • Cell phone Facebook app • Cell phone Twitter app • Cell phone Instagram app

Affiliation	System Type	Operational System
		• Cell phone Signal app
	Computer / Data	• E-mail content • *SMS messages* • *Facebook content* • *Twitter content* • *Signal messages*
	Communications	• Cell phones • Wi-Fi network • Marine Radio equipment
	Sensors	• Navigation radar
	Sensors / Human	• Visual (binoculars)
	Sensors / Cyber	• Digital Defences at network gateways (COTS anti-virus, threat detection)
	Effectors / Cyber	• *Malware*
	Platforms	• VOI • Ashore sites
Neutral	Human	• Fisherman
	Computer / Applications	• Facebook web service • Twitter web service • Instagram web service
	Computer / Data	• Facebook content • Twitter content • Instagram content
	Communications	• Cell phone network • Internet • Marine Radio equipment
Training	Human	• Instructor

4 ARCHITECTURE FUNCTIONALITY

4.1 Previous Work

In April 2016, prior to the task that produced this report, a multi-national workshop was held to investigate extending existing (legacy) CGF capabilities to include information warfare capabilities. A number of conceptual models were developed during and after the workshop that were used to evolve a four-layer architecture (Hazen, Lloyd, & Harris, The Evolution of Computer Generated Forces (CGF) Architectures to Support Information Warfare Effects, 2016). The resulting architecture is shown in Figure 4-1.

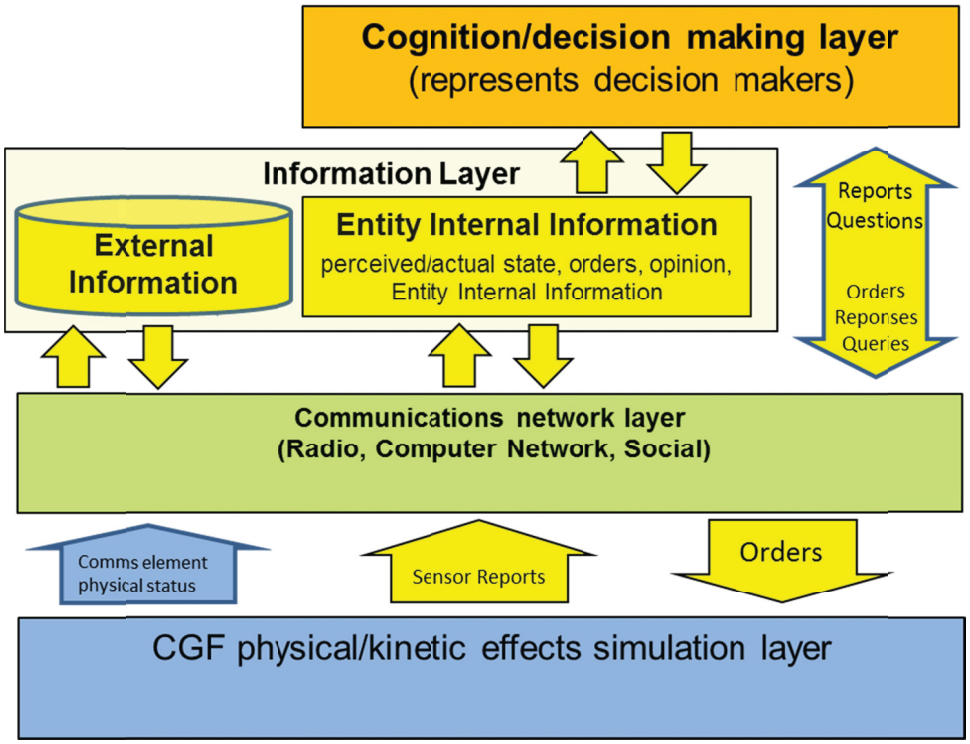

Figure 4-1: Information Warfare Engagement Model Architecture[1]

In this IW conceptual model, the central nature of the communications network layer is represented via the addition of information flows through it. Within the information layer, it acknowledges the separation of internal entity information (knowledge) and external information sources. It assumes that entities only communicate via the communications network layer. It also makes the assumption that all knowledge of the physical layer is generated by sensors via reports transmitted through a communications network.

[1] (Hazen, Lloyd, & Harris, The Evolution of Computer Generated Forces (CGF) Architectures to Support Information Warfare Effects, 2016)

What is less clear in the architecture is the separation of sensed simulation information (perceived state, represented the yellow arrows) from ground truth simulation data (truth state represented by the blue arrow). For example, while all simulated (perceived) entity knowledge of the physical layer must pass through the communications network layer, the communications network layer itself has a need for knowledge of the (truth) positions of communication network elements within the physical layer in order to adjudicate the state of communications links. Confusion between truth and (perceived) entity knowledge has occasionally caused problems in legacy CGF and so in this report we explicitly add and consider simulation truth data.

In this architecture, IW activities are initiated from the cognition layer and implemented by units who have a presence in the physical layer, but the IW activities take effect in either the communications network layer itself (e.g., jamming, denial of service) or within the elements of the information layer (e.g., changes to data, filtering of reports with respect to biases). However, the ultimate effect of the operations is to change the adversary's activities in the cognition layer with observable effects in the behaviour of units in the physical layer (e.g., changes to their position, posture, direction and rate of movement).

4.2 Enhanced Architecture

In Figure 4-2 we provide an enhanced version of the architecture diagram of Figure 4-1 to show examples of the components, information and effects that are modelled in each layer. Hereafter we refer to this as the IWSA. Two of the layers have been renamed compared to Figure 4-1, the information layer to content layer and the communications network layer to conduit layer, following feedback on an earlier version of Figure 4-2 presented in (Hazen, Harris, & Lamoureux, Extending Computer Generated Forces (CGF) Architectures to Support Information Warfare and Cyber Effects, 2017). In this section we discuss each of the layers in terms of their general content, and then each of the effects that apply to them.

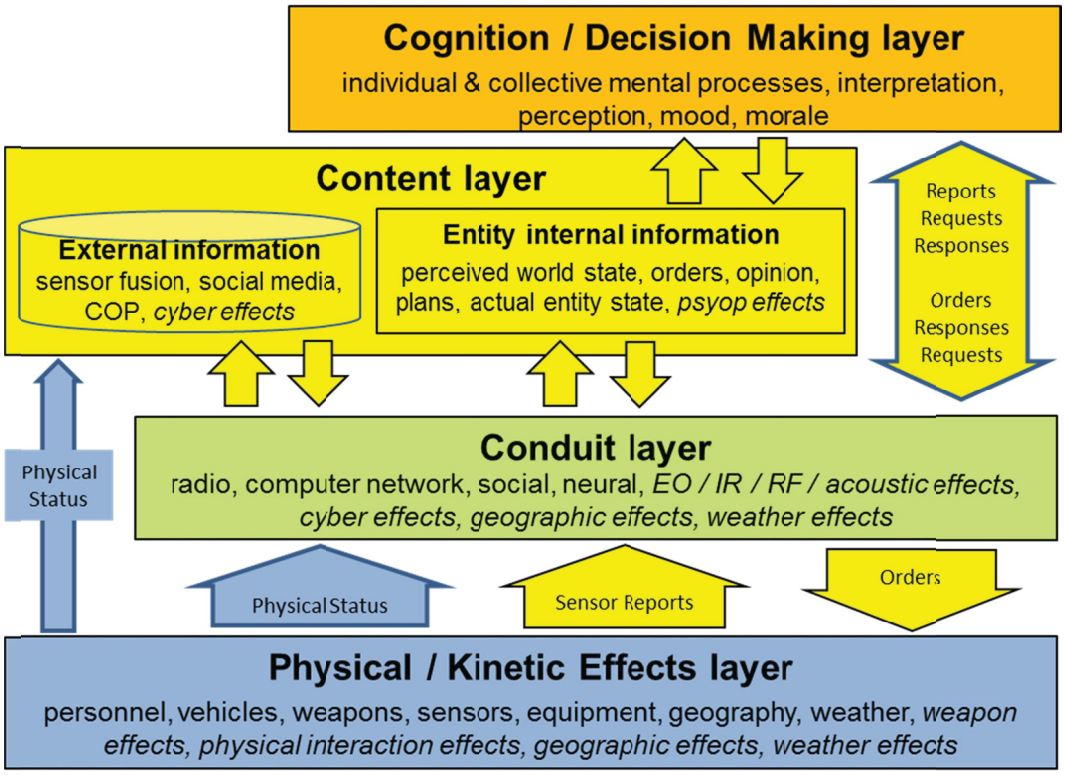

Figure 4-2: Enhanced Information Warfare Simulation Architecture

4.2.1 Layers

The four layers of the IWSA are: the Physical (Kinetic Effects) layer, the Conduit layer, the Content layer, and the Cognition (Decision Making) layer.

NOTE:	None of these layers specify or define a particular level of abstraction or fidelity for its components.

4.2.1.1 Physical/Kinetic Effects Layer

The Physical (Kinetic Effects) layer contains all of the elements of the physical world and the physical interactions between them. This includes the physical representation of personnel, vehicles and equipment. It includes weapons and sensors carried by and integrated in those platforms, and those that are standalone. Each of these components may be aggregated, individual or decomposed into sub-components. From a military affiliation standpoint, the components may be friendly, hostile or neutral.

The Physical layer also includes geographic and environmental elements such as terrain, buildings and other fixed installations, bodies of water (e.g., oceans, seas, lakes and rivers) and the atmosphere (e.g., weather).

The Physical layer encapsulates effects impacting elements in the layer. These effects are discussed in Section 4.2.2.

4.2.1.2 Conduit Layer

The Conduit layer contains all of the communications networks, the communications and networking elements (nodes) and the data that flows between the nodes. It encapsulates different types of communication and transmission media, including radio, intercom, satellite, computer networks, and social (media) networks. It does not include the physical manifestation of the communications elements, such as the transmitters, receivers and antennas, which are located in the Physical layer (but the components do receive physical manifestation status information when required). Similarly, it does not include the meaning of the payload data, which is located in the Content layer.

Computer applications, systems and services built upon them may be considered to be a part of the Conduit layer if they are involved in communicating content from one location to another. For example, the operating system embedded in a router is considered to be part of the Conduit layer. E-mail and web services, including server and client applications but not actual content, are also considered to be part of the Conduit layer.

The Conduit layer links the Physical layer to the Content and Cognition layers. A sensor (e.g., a radar) in the Physical layer will transmit information across a network in the Conduit layer (e.g., a computer network) to the Content layer for a sensor operator. The logical extension of this is to treat the neural pathways of an individual as a communications network of the Conduit layer. This then allows human optical and acoustic sensors (eyes and ears) modelled in the Physical layer to transmit information to be added to the Content layer. Whether this level of fidelity in the modelling is necessary and useful is another question entirely; for typical applications such information generated in the Physical layer will be directly transmitted to the Content layer.

The Conduit layer encapsulates effects impacting elements in the layer. These effects are discussed in Section 4.2.2.

4.2.1.3 Content Layer

The Content layer contains perceived and actual information content associated with humans and aggregate entities containing humans (entity internal information), and also technological information repositories and information processing systems such as computers and databases (external information). These sources of information are shown as *Entity Internal Information* and *External Information* respectively in Figure 4-2.

External Information includes the information content of messages in the Conduit layer, such as social media content related to social media networks; and processed and interpreted data received from the Physical layer such as fusion of sensor data and the production of a resulting COP.

Computer applications, systems and services built upon them may be considered to be a part of the Content layer if they are involved in creating or processing content. For example, the

operating system and application in a server creating and maintaining a COP is considered to be part of the Content layer. As a result, whether computer systems and applications belong to the Content or Conduit layers depends on their purpose. Additionally, different aspects of the computer systems and applications could belong to each layer, so holistically they could be regarding as belonging to both layers.

In the case of the simulation of humans, Entity Internal Information consists of both knowledge that is static and does not change, and the knowledge that may change as a scenario unfolds, including the state of the world as perceived by the entity, the actual state of the entity itself, and other information required to make decisions by models in the Cognition layer, such as plans, opinions and orders.

The Content layer encapsulates effects impacting elements in the layer. These effects are discussed in Section 4.2.2.

4.2.1.4 Cognition/Decision Making Layer

The Cognition (Decision Making) layer contains all of the individual and collective decision making processes, and associated interpretation of static and dynamic knowledge (knowledge that does not and does change throughout the scenario, respectively). It also contains psychological factors such as morale and mood that is, in part, derived from the knowledge present in the Entity Internal Information of the Content layer.

A team may be modelled as either a single unit or a group of units in the Cognition layer. The former will act like a single decision maker based on its static and dynamic knowledge, while the latter will act like a group of decision makers who must share information to make decisions.

Non-human systems that are sufficiently sophisticated to make complex decisions, either now or in the future, are also considered to be part of the Cognition layer. As a result, all decision making that effects change that is important to achieve a scenario objective is considered to be part of the Cognition layer, regardless of the source of the decision.

Within the IWSA, there are nominally no primary effects that affect the Cognition layer as it pertains to modelling humans. However, an information processing system that acts as a decision maker may be subject to cyber attack. Additionally, effects in the other layers will have a secondary or tertiary effect on the Cognition layer. These effects are discussed in Section 4.2.2.

4.2.1.5 Multi-Layer Elements

An element may be represented in multiple layers within the IWSA. For example, a communications tower will have components that are represented in the Physical and Conduit layers, for the physical manifestation of the tower and its presence as a node in communications networks, respectively. A computer database system may have components that are represented in the Physical, Conduit and Content layers, for the physical computer, as a computer network node, and the database content, respectively. Similarly, a human decision maker may have components in each of the four layers.

4.2.1.6 Entity Internal Information as a part of the Content or Cognition Layers

Within the conceptual IWSA, Entity Internal Information as it pertains to humans (for example, memory) is considered to be part of the Content layer.

A possible alternative representation would be to consider the Entity Internal Information as part of the Cognition layer, as it represents the “memory” and “knowledge” elements of human decision making and therefore should (arguably) be grouped together. It would then more closely align the architecture with the most likely implementation of decision maker models, in which the algorithms implementing decision maker and the data being operated on are all part of the same model.

However, in our view, a particular implementation of a model in software should not be the primary consideration in the development of the architecture. It is more important to group the architectural elements into a logically consistent structure, and we have included all information, knowledge and data content in the Content layer regardless of whether it is stored or just transmitted or recorded. In addition, we note that a particular implementation of a decision making model may well also have a presence in the Physical layer (e.g., the location of the decision maker) and potentially the Conduit layer (e.g., for verbal communication).

4.2.2 Effects

Figure 4-2 contains examples of the effects that can impact on each of the different layers in the IWSA. In the diagram, the effects are associated with the layers in which their primary impact is felt. Table 4-1 expands on this to show the different types of effects and the degree to which they can impact on each layer of the architecture.

Table 4-1: Effects Modelling in the IWSA

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

4.2.2.1 Weapon and Physical Interaction Effects

In this report, we assume weapon effects are the effects resulting from the use (e.g., detonation) of ballistic and other physical weapons. We define physical interaction effects (e.g., collisions) to be the effects resulting from interactions causing physical damage between non-weapon components in the physical layer. As a result, although there are differences in their genesis, weapon effects and physical interaction effects are very similar in terms of the impact that they have on the different layers in the IWSA.

Weapon and physical interaction effects primarily occur in the Physical layer, as this is their source. They can have a secondary effect in the Conduit layer, if communications components or infrastructure are damaged or destroyed in the Physical layer. Similarly, they can have a secondary effect in the Content layer if content-holding components in the Content layer (including both computer systems and humans) are physically damaged or destroyed in the Physical layer.

Weapon and physical interaction effects can have a tertiary effect in the Content layer through a secondary effect on the Conduit layer disrupting the transmission of content. Similarly, they can have a tertiary effect in the Cognition layer in the form of impaired decision making due to missing, incomplete or inaccurate information caused by secondary or tertiary effects in the Content layer, or reduced morale resulting from an accurate perception of changes in the Physical or Conduit layer.

4.2.2.2 Geographic and Weather Effects

Geographic effects and weather effects are both caused by models of the environment that are present in the Physical layer. Geographic effects include the effects of terrain and the ocean in terms of their presence, such as hills and rivers, and changes within them, such as fire, flood, earthquake and tsunami. Weather effects primarily occur in the atmosphere, but they can also result in secondary effects on the ground and on bodies of water, such as wind contributing to sea state.

Geographic and weather effects primarily occur in the Physical layer through changes to or the effects of the physical environment and the components (e.g., vehicles, humans and installations) within it. They can also have a primary effect in the Conduit layer. For example, radio and other communication can be impacted by both terrain (line of sight) and atmospheric (weather) conditions.

Geographic and weather effects can have a follow-on secondary effect in the Content layer if sensors in the Physical layer or communication means in the Conduit layer are impacted by the geographic or weather effects. Similarly, there can be a tertiary effect in the Cognition layer in the form of impaired decision making due to missing, incomplete or inaccurate information content caused by secondary effects in the Content layer, or reduced morale resulting from an accurate perception of significant changes in the Physical layer.

4.2.2.3 EO/IR/RF/Acoustic Effects

While the Electro-Optical (EO) / Infrared (IR) / Radio Frequency (RF) / Acoustic effects are most likely to be related to Electronic Warfare (that is, RF), similar effects may come from EO, IR and acoustic based systems and we expect them to be modelled in the same way.

Electronic Warfare effects involve offensive (EA), defensive (EP) and support (ES) activities in the electromagnetic spectrum. As such, they are considered to take place primarily in the Conduit layer.

Some EA activities such as radar jamming can affect the radar sensors in the Physical layer as a secondary effect and therefore the Content and Cognition layers as tertiary effects. Others, such as radio/communications jamming can affect the Content layer as a secondary effect.

Similarly, EP activities intended as protection against sensors can affect those sensors in the Physical layer as a secondary affect, and therefore the Content and Cognition layers as tertiary effects.

ES activities such as electronic intelligence (ELINT) and SIGINT will also affect sensors in the Physical layer as a secondary affect and then the Content and Cognition layers as tertiary effects.

Table 4-2 contains a summary of the different EW effects and the impact they have on the different layers in the IWSA.

Table 4-2: EW Effect Modelling in the IWSA

EW Effect	Physical	Conduit	Content	Cognition
Electronic Attack	Secondary	Primary	Secondary or Tertiary	Tertiary
Electronic Protection	Secondary	Primary	Tertiary	Tertiary
Electronic Warfare Support	Secondary	Primary	Tertiary	Tertiary

4.2.2.4 Cyber Effects

Cyber effects can take place primarily in the Conduit and Content layers, depending upon the particular attack type and resulting cyber effect. Table 4-3 shows the different types of cyber effects, as defined by Musman et al. (Musman, Temin, Tanner, Fox, & Pridmore, 2010) and considered by Bernier (Bernier, 2013), and the impact they may have on each of the different layers in the IWSA.

Table 4-3: Cyber Effect Modelling in the IWSA

Cyber Effect	Physical	Conduit	Content	Cognition
Interruption	Tertiary	Primary	Primary	Secondary & Primary
Modification	Tertiary	Secondary	Primary	Secondary
Degradation	Tertiary	Primary	Primary	Secondary & Primary
Fabrication	Tertiary	Secondary	Primary	Secondary
Interception	Attacker Tertiary	Primary	Primary	Attacker Secondary & Primary
Unauthorized Use	Secondary	Primary	Primary	Tertiary & Primary

The cyber effect of Interruption occurs primarily in the Conduit and Content layers. For example, in the Conduit layer, a denial-of-service attack can result in an interruption to the delivery of data across a network. In the Content layer, the management and processing of data can be interrupted using attack vectors such as viruses and rootkits. Note that the attack vector may involve the Physical layer. For example, in the Physical layer, sabotage may result from physical access to the equipment or its environment. However, as the cyber effect that results from this attack vector will be modelled in the Conduit or Content layer, we do not consider that the cyber effect occurs in the Physical layer. These attacks can have secondary effects on decision-making in the Cognition layer reflected in time-late information and loss of trust. The tertiary effects can be seen by frustration in units not getting responses to queries and implementing alternative communications or executing local operations. If the Cognition layer represents a computer system performing the decision making, then the cyber effect of Interruption can also occur primarily in the Cognition layer in a manner similar to attack vectors in the Content layer.

The cyber effect of Modification will primarily occur in the Content layer, but can also result from an attack in the Conduit layer. Although network payload data can be altered in the Conduit layer, it is the Content layer that gives the data its meaning and therefore, from a practical standpoint, the Content layer is where Modification must primarily be modelled. In addition, the effect of Modification may occur entirely within the Content layer through attacking the management and processing of data using attack vectors such as viruses and rootkits. Secondary effects can be seen in changed network configurations within the Conduit layer, and lack of trust, bias reinforcement and confusion in the Cognition layer. Tertiary effects can be seen in the Physical layer in changes in behaviour of units resulting from the effects in the Cognition layer.

The cyber effect of Degradation will also primarily occur in the Conduit and Content layers. In the Conduit layer, a denial-of-service attack may degrade communications services and reduce network performance. In the Content layer, processing of data may be degraded by attacks on the computer operating system and its services using attack vectors such as viruses and rootkits. As for the cyber effect of Interruption, the attack vector may involve the Physical layer. Again, as the cyber effect that results from this attack vector will be modelled in the Conduit or Content layer, we do not consider that the primary cyber effect occurs in the Physical layer. Secondary effects can occur in the Cognition layer as it loses trust or has biases reinforced, and

tertiary effects can be seen in the Physical layer as command and control degrades and unit operations lose cohesion. If the Cognition layer represents a computer system performing the decision making, then the cyber effect of Degradation can also occur primarily in the Cognition layer in a manner similar to attack vectors in the Content layer.

For the purposes of the IWSA, in many ways the cyber effects of Fabrication are similar to Modification, except that instead of modifying information content, additional data (information content) is inserted into a system. Note that, unlike Modification, the attack vector for Fabrication can involve the Cognition layer by attempting to get a decision maker to trigger the fabrication in error via techniques such as phishing. However, as the cyber effect that results from this attack vector will be modelled in the Content layer, we do not consider that the primary cyber effect occurs in the Cognition layer. Secondary and tertiary effects are similar to Modification.

The cyber effect of Interception can occur in the Conduit and Content layers. For example, it may be modelled in the Conduit layer through the interception of network data communications, and in the Content layer through an attack on the management and processing of data. As in the case of Fabrication, Interception of information content can also involve the Cognition layer using an attack vector that attempts to get a decision maker to trigger the transmission of information in error via techniques such as phishing. Again, although this variation of attack will involve the Cognition layer, as the cyber effect that results from this attack vector will be modelled in the Content layer, for this case we do not consider that the primary cyber effect occurs in the Cognition layer. Secondary and tertiary effects can occur in the attacker's Cognition and Physical layers as they change their decision-making and behaviour (or not) to take advantage of the information intercepted. If the Cognition layer represents a computer system performing the decision making, then the cyber effect of Interception can also occur primarily in the Cognition layer in a manner similar to attack vectors in the Content layer.

The cyber effect of Unauthorized Use (control of physical, information and network assets) will primarily occur in the Conduit and Content layers where new communications channels are established, and system configuration and control data are changed. Secondary effects can be seen in changed behaviour of the resource in the Physical layer as it responds to the new command chain. Tertiary effects can be seen in the Cognition layer as the former owner realizes its loss of control and reacts. If the Cognition layer represents a computer system performing the decision making, then the cyber effect of Unauthorized Use can also occur primarily in the Cognition layer in a manner similar to attack vectors in the Content layer.

4.2.2.5 Psychological Operations Effects

Psychological Operations (PSYOP) are aimed at influencing the behaviour of humans, be it individually or in groups, and decision making through information. As such, PSYOP effects primarily occur in the Content layer and target shaping the Entity Internal Information.

Secondary effects occur in the Cognition layer as a result of the shaped information, resulting in changed decision making. This decision making results in tertiary effects in the Conduit and Physical layers.

4.2.3 Modelling Use of Truth Data

The architecture in Figure 4-2 combines 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.

While perceived data and truth data are distinct concepts, we note that equating truth and perceived data within a particular simulation can also be a valid modelling technique for particular levels of fidelity and desired modelling capability. In all cases we believe that doing this should be a conscious decision based on the needs of the simulation. However, actually equating them (for example, using one set of variables to represent both concepts) in design and implementation can be a very constraining (bad) design decision, as it limits future maintainability and harms the prospects for easy reuse in different circumstances. A more flexible and maintainable design would store them separately even if they are equated in an initial implementation so that they can be separated later if the need arises.

4.2.4 Live, Virtual and Constructive

While our primary use for the IWSA is to propose extensions to CGF architectures (which are, depending on the application, virtual or constructive) to support IW, the architecture is applicable to all elements and instances of 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 that an agent-based red force opponent behavioural model is.

4.3 Use Case

We now employ the use case presented in Section 3.3 to demonstrate how the modelling of operational systems and (some) data is distributed in the IWSA.

Table 4-4 contains a mapping of the operational systems (and some data) in the Present OCO Simulation use case listed in Table 3-5 to the four layers of the IWSA. Where an operational system is represented in a layer, we provide an example of the role that the system plays or the data that it encapsulates in that layer.

Operational systems shown in italics in Table 4-4 are not directly mentioned in the steps of the Present OCO Simulation use case in Section 3.3 but are included for completeness.

For each system, Table 4-4 also indicates whether the system will be simulated by a Live (L), Virtual (V) or Constructive (C) component in the simulation. Systems listed as being simulated by a Constructive component are assumed to be simulated by the CGF. Systems listed as being simulated by a Live component are assumed to be simulated by the actual people or equipment, while systems listed as being simulated by a Virtual component are assumed to be simulated by simulated (physical) equipment or systems. The Live components are the CTG Staff, while the equipment that they directly interact with are assumed to be either Live or Virtual components.

Note that for a given level of fidelity, not all of the operational systems in Table 4-4 will need to be represented in all layers. For example, while the Internet network is composed of many physical components with specific locations (computers, routers, cables, etc.), they are not required to be present in the Present OCO Simulation use case scenario.

Table 4-4: Mapping of Operational Systems in Present OCO Simulation Use Case to IWSA Layers

Operational System / Data	LVC	Physical	Conduit	Content	Cognition
Friendly					
CTG Staff	L	Location		Knowledge	Decision making
IW Resources staff	C	Location		Entity Internal Info	Decision making
EW Resources staff	C	Location		Entity Internal Info	Decision making
Joint HQ staff	C	Location		Entity Internal Info	Decision making
CTG Staff computers	L or V	Location	Network node & processing	Processing & storage	
CTG Staff network (servers, routers)	L or V	Location	Network nodes, connections & processing	Configuration	
IW Resources computers	C	Location	Network node & processing	Processing & storage	
IW Resources network (servers, routers)	C	Location	Network nodes, connections & processing	Configuration	
EW Resources computers	C	Location	Network node & processing	Processing & storage	
EW Resources network (servers, routers)	C	Location	Network nodes, connections & processing	Configuration	
Joint HQ computers	C	Location	Network node & processing	Processing & storage	
Joint HQ network (servers, routers)	C	Location	Network nodes, connections & processing	Configuration	
CTG Staff e-mail system	L or V	Location	E-mail clients & servers	E-mail content	
CTG Staff chat system	L or V	Location	Chat clients & servers	Chat content	

Operational System / Data	LVC	Physical	Conduit	Content	Cognition
IW Resources e-mail system	C	Location	E-mail clients & servers	E-mail content	
IW Resources chat system	C	Location	Chat clients & servers	Chat content	
EW Resources e-mail system	C	Location	E-mail clients & servers	E-mail content	
EW Resources chat system	C	Location	Chat clients & servers	Chat content	
Joint HQ e-mail system	C	Location	E-mail clients & servers	E-mail content	
IW Resources Facebook app	C		Web node	Web content	
IW Resources Twitter app	C		Web node	Web content	
IW Resources Instagram app	C		Web node	Web content	
Website #1 containing Malware	C		Web node	Web content	
Website #2 contacted by Malware	C		Web node	Web content	
CTG Staff e-mail content	L or V		Transport	Data	Trust
CTG Staff chat content (saved)	L or V		Transport	Data	Trust
IW Resources e-mail content	C		Transport	Data	Trust
IW Resources chat content (saved)	C		Transport	Data	Trust
EW Resources e-mail content	C		Transport	Data	Trust
EW Resources chat content (saved)	C		Transport	Data	Trust
Joint HQ e-mail content	C		Transport	Data	Trust
Facebook content	C		Transport	Data	Trust
Twitter content	C		Transport	Data	Trust
Instagram content	C		Transport	Data	Trust
CTG Staff LAN	L or V	Locations	Nodes & connections	Configuration	

Operational System / Data	LVC	Physical	Conduit	Content	Cognition
IW Resources LAN	C	Locations	Nodes & connections	Configuration	
EW Resources LAN	C	Locations	Nodes & connections	Configuration	
Joint HQ LAN	C	Locations	Nodes & connections	Configuration	
TG WAN	C	Locations	Nodes & connections	Configuration	
Commercial Internet access	C	Locations	Nodes & connections	Configuration	
IW Resources cell phones	C	Locations	Nodes, connections & processing	Processing & storage	
Marine Radio equipment	C	Locations	Nodes & connections		
SATCOM	C	Locations	Nodes & connections		
AIS	C	Locations	Nodes & connections		
Navigation radar	C	Location & sense[2]	Network node		
Tracking radar	C	Location & sense	Network node		
Sensor fusion	C		Network node	Processing & storage	
EOIR detect and track	C	Location & sense	Network node		
Visual	C	Location & sense			
HUMINT	C	Location		Knowledge	Conversation / interrogation
COMINT sensor	C	Location	Sense		
ELINT sensor	C	Location	Sense		
SIGINT sensor	C	Location	Sense		

[2] Sense covers detection, tracking, classification, identification as applicable based on the capabilities of the sensor.

Operational System / Data	LVC	Physical	Conduit	Content	Cognition
Digital defences at network gateways (IDS, virus scanners)	C			Applications	
User reporting procedures for system irregularities	C			SOPs	
Social media tracking	C		Transport	Data	Interpretation & decision making
Malware	C			Application	
Jammer	C	Location	Jam		
TG ships: CTG Staff ship, IW Resources ship, EW Resources ship	C	Locations, sensors & weapons			
Hostile					
Adversary	C	Location		Entity Internal Info	Decision making
Adversary colleagues	C	Location		Entity Internal Info	Decision making
Laptops	C	Location	Network node & processing	Processing & storage	
Cell phone e-mail client	C		E-mail client	E-mail content	
Cell phone web browser	C		Web node	Web content	
Cell phone Facebook app	C		Web node	Web content	
Cell phone Twitter app	C		Web node	Web content	
Cell phone Instagram app	C		Web node	Web content	
Cell phone Signal app	C		Cell phone & Wi-Fi network node	Message content	
E-mail content	C		Transport	Data	

Operational System / Data	LVC	Physical	Conduit	Content	Cognition
SMS messages	C		Transport	Data	
Facebook content	C		Transport	Data	
Twitter content	C		Transport	Data	
Signal messages	C		Transport	Data	
Cell phones	C	Location	Cell phone & Wi-Fi network nodes & processing	Processing & storage	
Phone conversation (spoken messages)	C			Data	
Wi-Fi network	C	Router locations	Nodes & connections	Configuration	
Marine Radio equipment	C	Location	Communication node		
Marine Radio (spoken) messages	C			Data	
Navigation radar	C	Location & sense			
Visual (binoculars)	C	Location & sense			
Digital Defences at network gateways (COTS AV & threat detection)	C			Applications	
Malware	C			Application	
VOI	C	Location			
Ashore sites	C	Location			
Neutral					
Fisherman	C	Location		Entity Internal Info	Decision making
Fishing boat	C	Location			

Operational System / Data	LVC	Physical	Conduit	Content	Cognition
Marine Radio equipment	C	Location	Communication node		
Marine Radio (spoken) messages	C			Data	
Facebook web service	C		Web service	Web content	
Twitter web service	C		Web service	Web content	
Instagram web service	C		Web service	Web content	
Facebook content	C		Transport	Data	
Twitter content	C		Transport	Data	
Instagram content	C		Transport	Data	
Cell phone network	C	Locations	Nodes & connections	Configuration	
Internet	C	Locations	Nodes & connections	Configuration	

5 ARCHITECTURE LAYER INTERFACES

There are a range of different factors that should be taken into account when considering the interfaces within and between the layers in an architecture. In this section, we leverage the Present OCO Simulation use case to motivate and consider the general and specific interfaces of the layers of the IWSA.

5.1 Use Case Component Interactions

The steps in the use case described in Section 3.3 are insufficiently detailed to directly describe the interactions between the various components (operational systems) listed in Section 4.3.

In this section, we first decompose each step in the Present OCO Simulation use case into activities performed by each operational system and significant piece of information. This will then enable us to make some observations with respect to the interactions and interfaces between components of different types and in different layers of the IWSA.

5.1.1 Each Step in the Use Case

5.1.1.1 Step 1

Consider Step 1 in the Present OCO Simulation use case: CTG Staff prepares an OCO plan. Table 5-1 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, only the Cognition and Content layers are involved, and the CTG Staff computer is regarded as part of the Content layer based on its role in preparing content.

Table 5-1: Operational Systems and Activities in Step 1

CTG Staff Prepares OCO Plan

Operation System and Activity	Type	Layer
CTG Staff formulates an *OCO plan*	Decision Information	Cognition Content
CTG Staff prepares an *OCO plan* using *CTG Staff computer*	Action Information Information System	Cognition Content Content

Figure 5-1 contains a representation of step 1 as a Unified Modeling Language (UML) communication diagram. The components in each layer are shown using the same colour. Each row in Table 5-1 corresponds to a set of messages in Figure 5-1 that are numerically linked and shown in the same colour (numbered 1 and black for the first row, and numbered 2 and brown for the second).

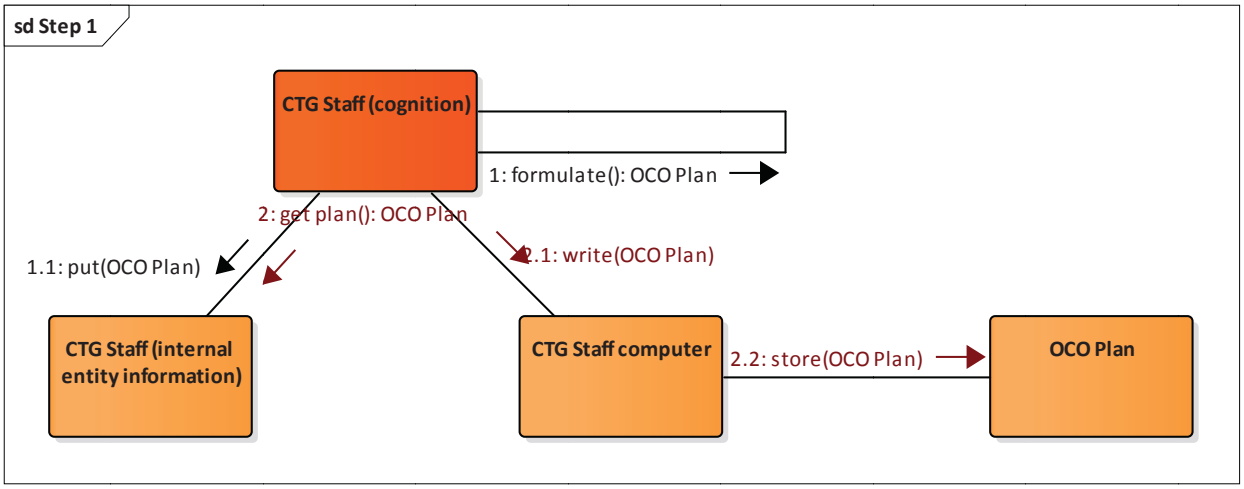

Figure 5-1: Communication Diagram for Step 1

CTG Staff Prepares an OCO Plan

5.1.1.2 Step 2

Consider Step 2 in the Present OCO Simulation use case: CTG Staff requests allocation of IW Resources from Joint HQ staff as a Subordinate Unit via e-mail. Table 5-2 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved. In contrast to the previous step, the CTG Staff computer is regarded as part of the Conduit layer based on its role in communicating content.

Table 5-2: Operational Systems and Activities in Step 2

CTG Staff Requests Allocation of IW Resources from Joint HQ Staff as a Subordinate Unit via E-Mail

Operation System and Activity	Type	Layer
CTG Staff decide to send e-mail requesting allocation of IW Resources as a Subordinate Unit	Decision Information	Cognition Content
CTG Staff create e-mail using *CTG Staff computer* and *CTG Staff e-mail system*, it is stored as *CTG Staff e-mail content*	Action Communication System Communication System Information	Cognition Conduit Conduit Content
CTG Staff sends created e-mail to addressee using *CTG Staff e-mail system* on the *CTG Staff computer*; *CTG Staff e-mail system* sends e-mail	Action Communication System Communication System Communication System	Cognition Conduit Conduit Conduit

Operation System and Activity	Type	Layer
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 takes *CTG Staff ship* and *Joint HQ* locations into account,	Location	Physical
Joint HQ LAN	Communication System	Conduit
which uses *Joint HQ Network* equipment,	Communication System	Conduit
to the *Joint HQ e-mail system*	Communication System	Conduit
on the *Joint HQ computer*,	Communication System	Conduit
the e-mail is stored as *Joint HQ e-mail content*	Information	Content

Figure 5-2 contains a representation of Step 2 as a UML communication diagram.

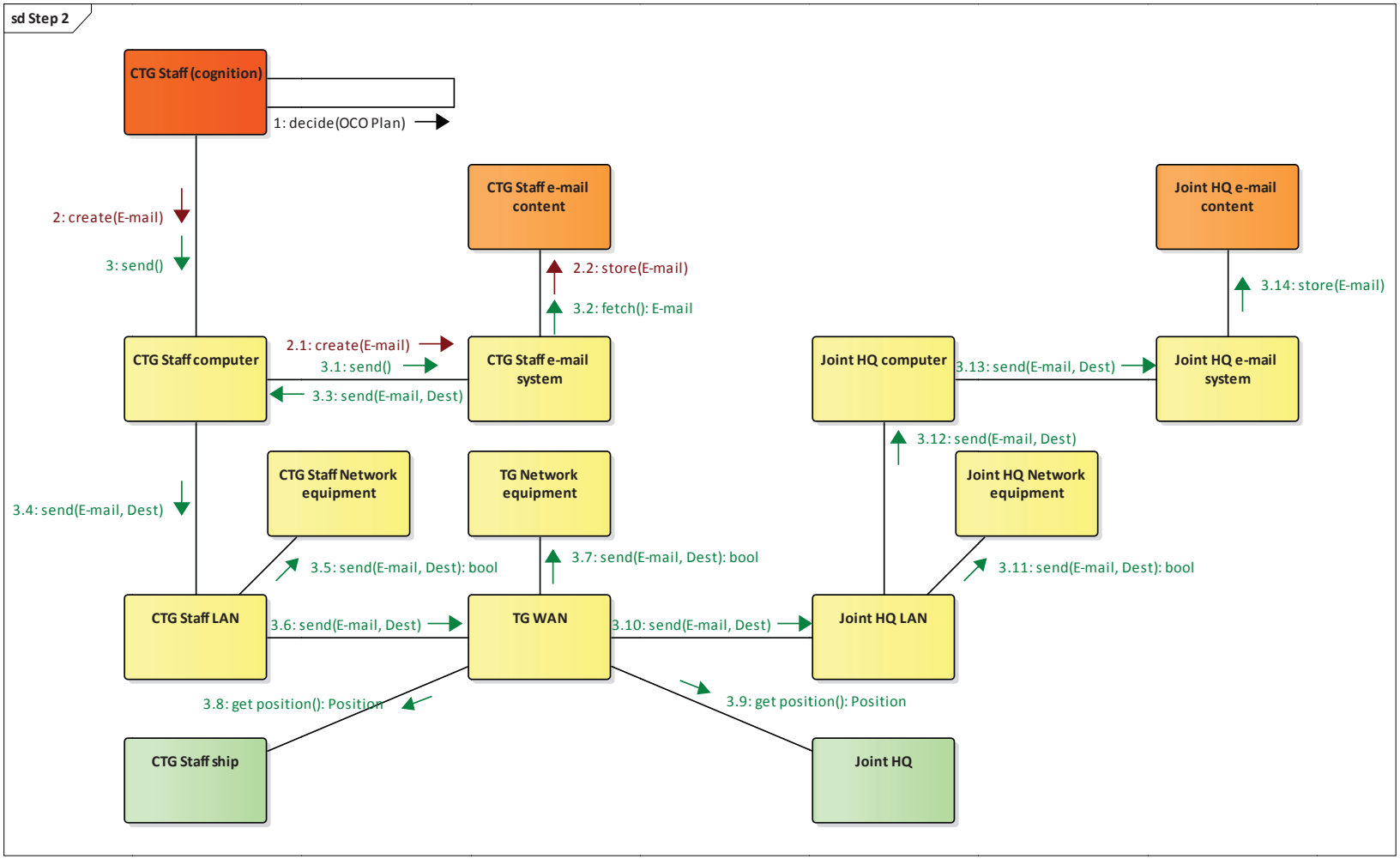

Figure 5-2: Communication Diagram for Step 2

CTG Staff Requests Allocation of IW Resources from Joint HQ Staff as a Subordinate Unit via E-Mail

5.1.1.3 Step 3

Consider Step 3 in the Present OCO Simulation use case: Joint HQ allocates IW Resources to CTG Staff via e-mail, changing the active organizational structure involving IW Resources. Table 5-3 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-3: Operational Systems and Activities in Step 3

Joint HQ Allocates IW Resources to CTG Staff via E-Mail, Changing Active Organizational Structure Involving IW Resources

Operation System and Activity	Type	Layer
Joint HQ staff reads the e-mail	Observe	Cognition
stored as *Joint HQ e-mail content*	Information	Content
using the *Joint HQ e-mail system*	Information System	Content
on the *Joint HQ computer*	Information System	Content
Joint HQ staff decides to allocate *IW Resources* to *CTG Staff*	Decide	Cognition
Joint HQ staff updates	Action	Cognition
the organizational structure	Information	Content
Joint HQ staff create e-mail	Action	Cognition
using *Joint HQ computer*	Communication System	Conduit
and *Joint HQ e-mail system*,	Communication System	Conduit
it is stored as *Joint HQ e-mail content*	Information	Content
Joint HQ staff sends created e-mail to addressees	Action	Cognition
using *Joint HQ e-mail system*	Communication System	Conduit
on the *Joint HQ computer*;	Communication System	Conduit
Joint HQ e-mail system sends e-mail	Communication System	Conduit
from *Joint HQ e-mail content*	Information	Content
routing it over *Joint HQ LAN*	Communication System	Conduit
which uses *Joint HQ Network* equipment,	Communication System	Conduit
TG WAN	Communication System	Conduit
which uses *TG Network* equipment	Communication System	Conduit
and takes *Joint HQ*, *CTG Staff ship* and *IW Resources ship* locations into account,	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

Operation System and Activity	Type	Layer
and *CTG Staff LAN*	Communication System	Conduit
which uses *CTG Staff Network* equipment,	Communication System	Conduit
to the *CTG Staff e-mail system*	Communication System	Conduit
on the *CTG Staff computer*,	Communication System	Conduit
the e-mail is stored as *CTG Staff e-mail content*	Information	Content
CTG Staff reads the e-mail	Observe	Cognition
stored as *CTG Staff e-mail content*	Information	Content
using the *CTG Staff e-mail system*	Information System	Content
on the *CTG Staff computer*	Information System	Content
IW Resources reads the e-mail	Observe	Cognition
stored as *IW Resources e-mail content*	Information	Content
using the *IW Resources e-mail system*	Information System	Content
on the *IW Resources computer*	Information System	Content

Figure 5-3 contains a representation of Step 3 as a UML communication diagram.

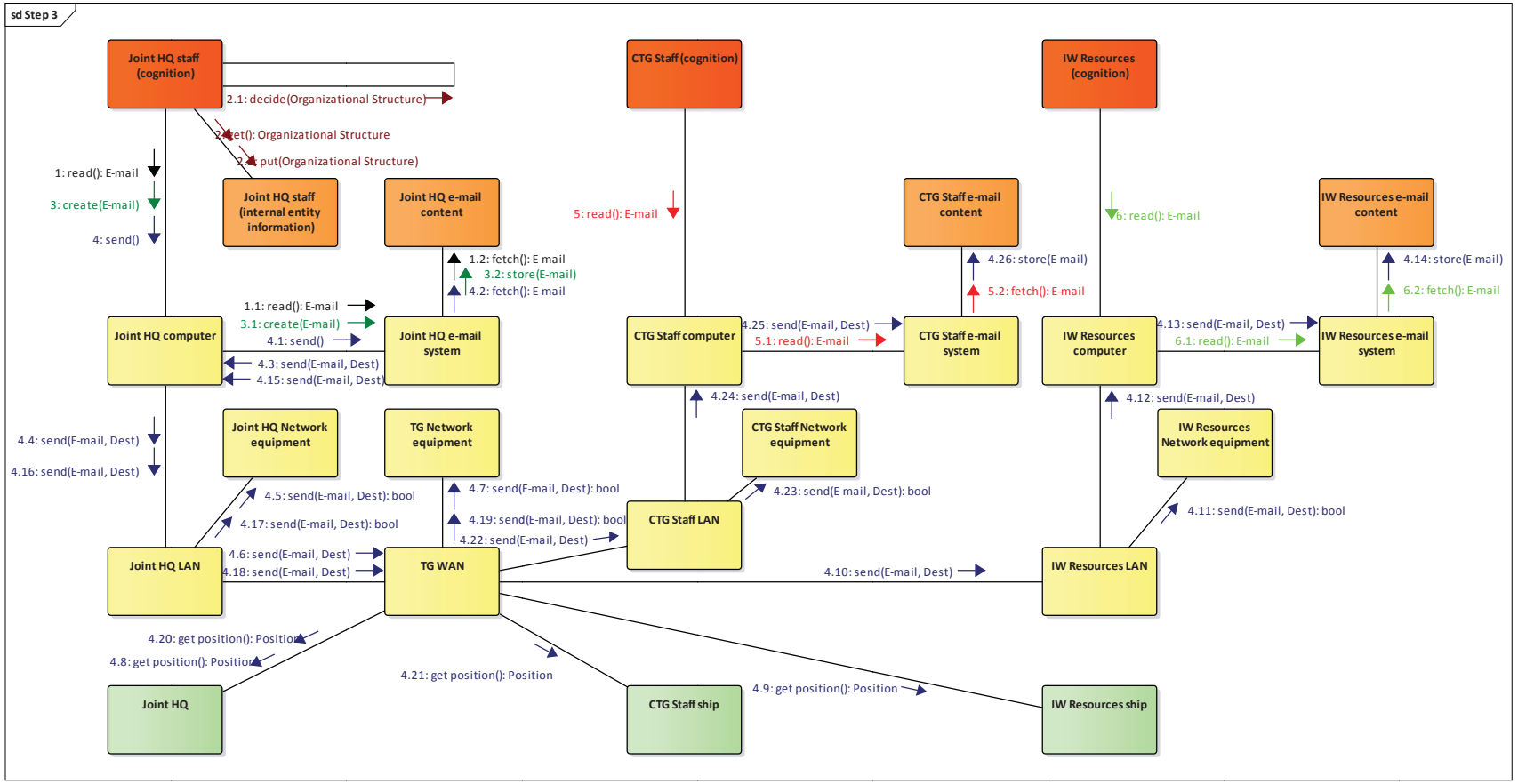

Figure 5-3: Communication Diagram for Step 3

Joint HQ Allocates IW Resources to CTG Staff via E-Mail, Changing Active Organizational Structure Involving IW Resources

5.1.1.4 Step 4

Consider Step 4 in the Present OCO Simulation use case: CTG Staff sends the OCO plan to Subordinate Unit (IW Resources and EW Resources) via e-mail. Table 5-4 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-4: Operational Systems and Activities in Step 4

CTG Staff Sends OCO Plan to Subordinate Unit (IW Resources) via E-Mail

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

Figure 5-4 contains a representation of Step 4 as a UML communication diagram.

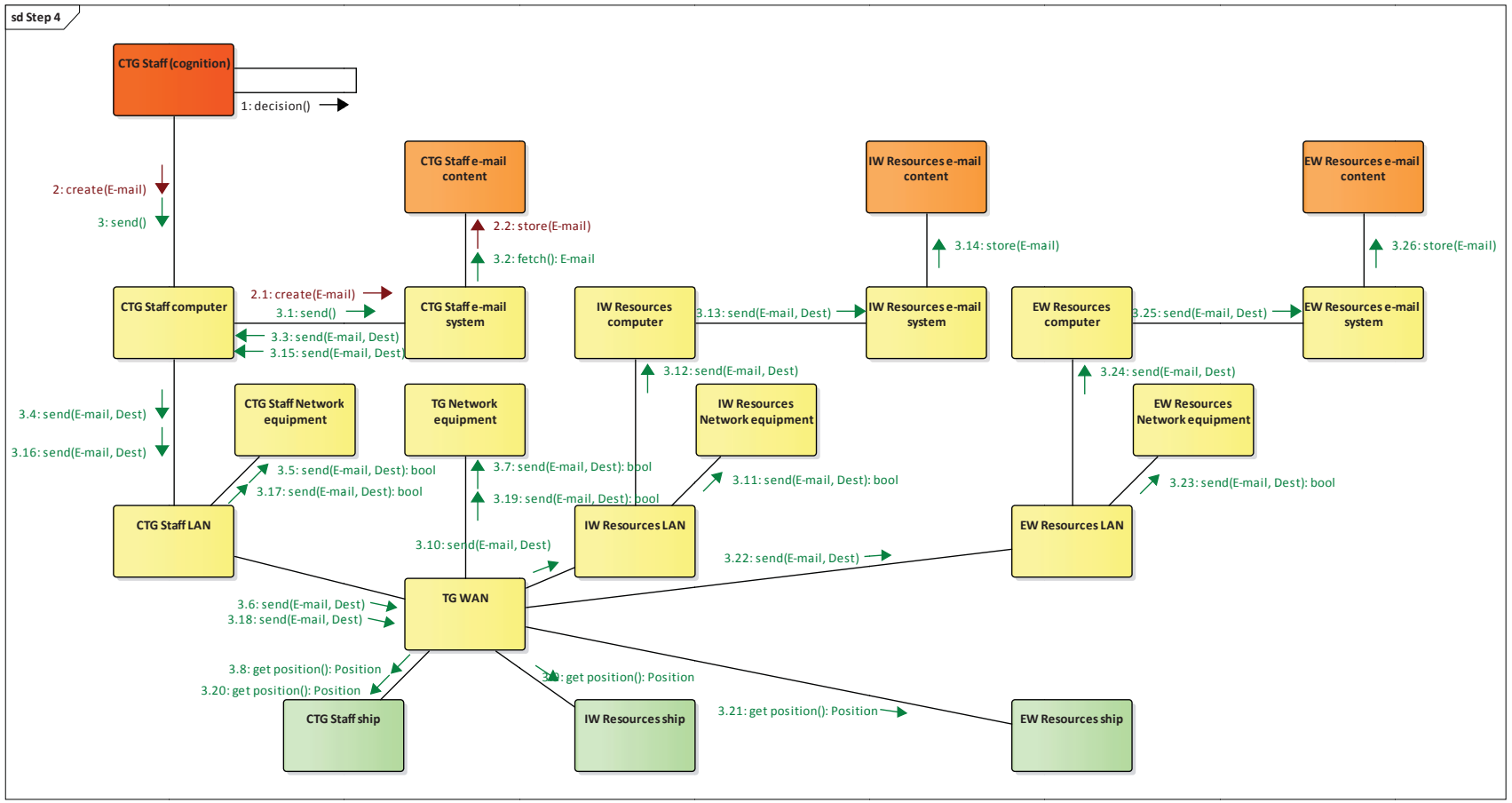

Figure 5-4: Communication Diagram for Step 4

CTG Staff Sends OCO Plan to Subordinate Unit (IW Resources and EW Resources) via E-Mail

5.1.1.5 Step 5

Consider step 5 in the Present OCO Simulation use case: IW Resources review the OCO plan. Table 5-5 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, only the Cognition and Content layers are involved.

Table 5-5: Operational Systems and Activities in Step 5

IW Resources Review OCO Plan

Operation System and Activity	Type	Layer
IW Resources reads the e-mail	Observe	Cognition
stored as *IW Resources e-mail content*	Information	Content
using the *IW Resources e-mail system*	Information System	Content
on the *IW Resources computer*	Information System	Content
IW Resources tries to understand and evaluates the completeness of	Orient	Cognition
the *OCO plan*	Information	Content
in the context of their opinions and cognitive biases	Information	Content

Figure 5-5 contains a representation of Step 5 as a UML communication diagram.

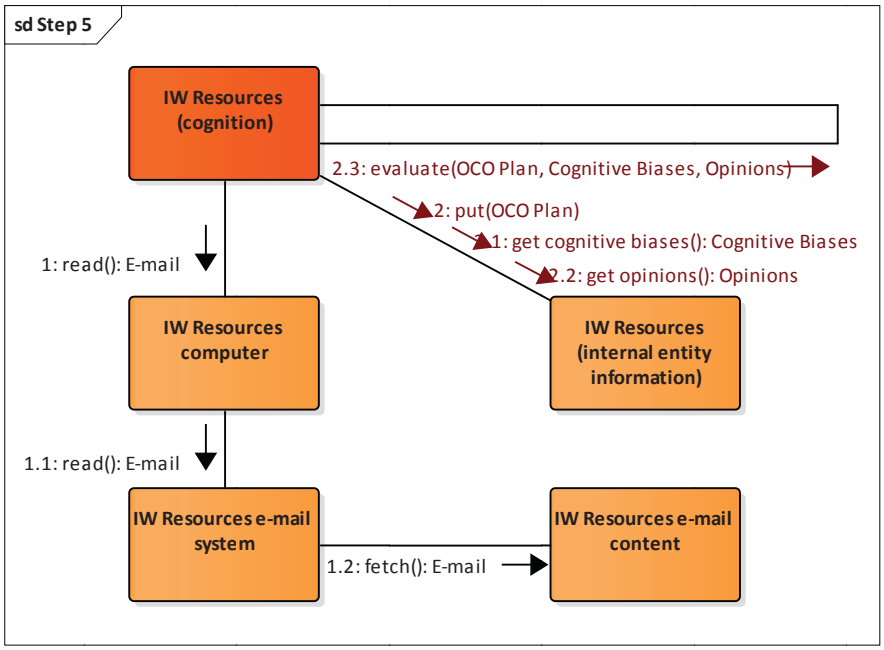

Figure 5-5: Communication Diagram for Step 5

IW Resources Review OCO Plan

5.1.1.6 Step 6

Consider Step 6 in the Present OCO Simulation use case: 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. Table 5-6 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-6: Operational Systems and Activities in Step 6

IW Resources Seek Clarification from CTG Staff on Type of Social Media, Nature of Cyber Attack, Effect to be Achieved, and Type of Cell Phones and Laptops Identified by HUMINT via Electronic Chat

Operation System and Activity	Type	Layer
IW Resources decide clarification is needed on the *OCO plan*	Decision Information	Cognition Content
IW Resources uses	Action	Cognition
the *IW Resources chat system*	Communication System	Conduit
producing *IW Resources chat content*	Information	Content
on the *IW Resources computer*,	Communication System	Conduit
which is sent via the *IW Resources LAN*,	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
via the *TG WAN*,	Communication System	Conduit
which uses *TG Network* equipment	Communication System	Conduit
and takes *CTG Staff ship* and *IW Resources ship* locations into account,	Location	Physical
and the *CTG Staff LAN*	Communication System	Conduit
which uses *CTG Staff Network* equipment,	Communication System	Conduit
to the *CTG Staff chat system*	Communication System	Conduit
on the *CTG Staff computer*,	Communication System	Conduit
and stores message as *CTG Staff chat content*	Information	Content
to ask about 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		

Figure 5-6 contains a representation of Step 6 as a UML communication diagram.

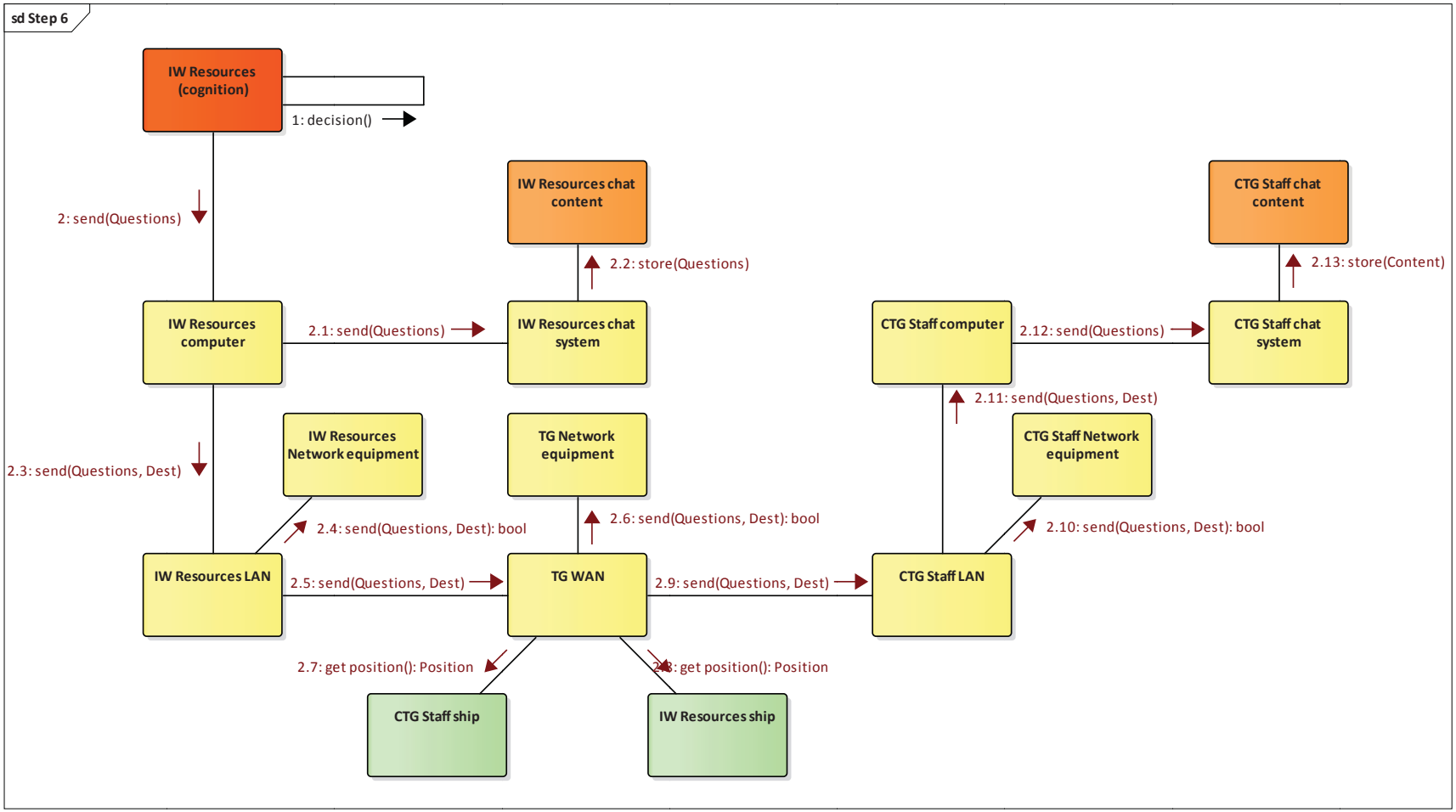

Figure 5-6: Communication Diagram for Step 6

IW Resources Seek Clarification from CTG Staff

5.1.1.7 Step 7

Consider Step 7 in the Present OCO Simulation use case: 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. Table 5-7 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-7: Operational Systems and Activities in Step 7

CTG Staff Clarifies OCO Plan via Electronic Chat: They Have no Preference with Respect to Type of Social Media or Nature of Cyber Attack, but They do Want to Have as Much Advanced Warning of Adversary's Movements as Possible to Facilitate Interception; CTG Staff also Provides Type of Cell Phones and Laptops Identified by HUMINT

Operation System and Activity	Type	Layer
CTG Staff decide how to clarify the *OCO plan*	Decision Information	Cognition Content
CTG Staff uses	Action	Cognition
the *CTG Staff chat system*	Communication System	Conduit
producing *CTG Staff chat content*	Information	Content
on the *CTG Staff computer*,	Communication System	Conduit
which is sent via the *CTG Staff LAN*,	Communication System	Conduit
which uses *CTG Staff Network* equipment,	Communication System	Conduit
via the *TG WAN*,	Communication System	Conduit
which uses *TG Network* equipment	Communication System	Conduit
and takes *CTG Staff ship* and *IW Resources ship* locations into account,	Location	Physical
and the *IW Resources LAN*	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
to the *IW Resources chat system*	Communication System	Conduit
on the *IW Resources computer*,	Communication System	Conduit
and stores message as *IW Resources chat content*	Information	Content
to answer that 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; they also provide the type of cell phones and laptops identified by HUMINT		

Figure 5-7 contains a representation of Step 7 as a UML communication diagram.

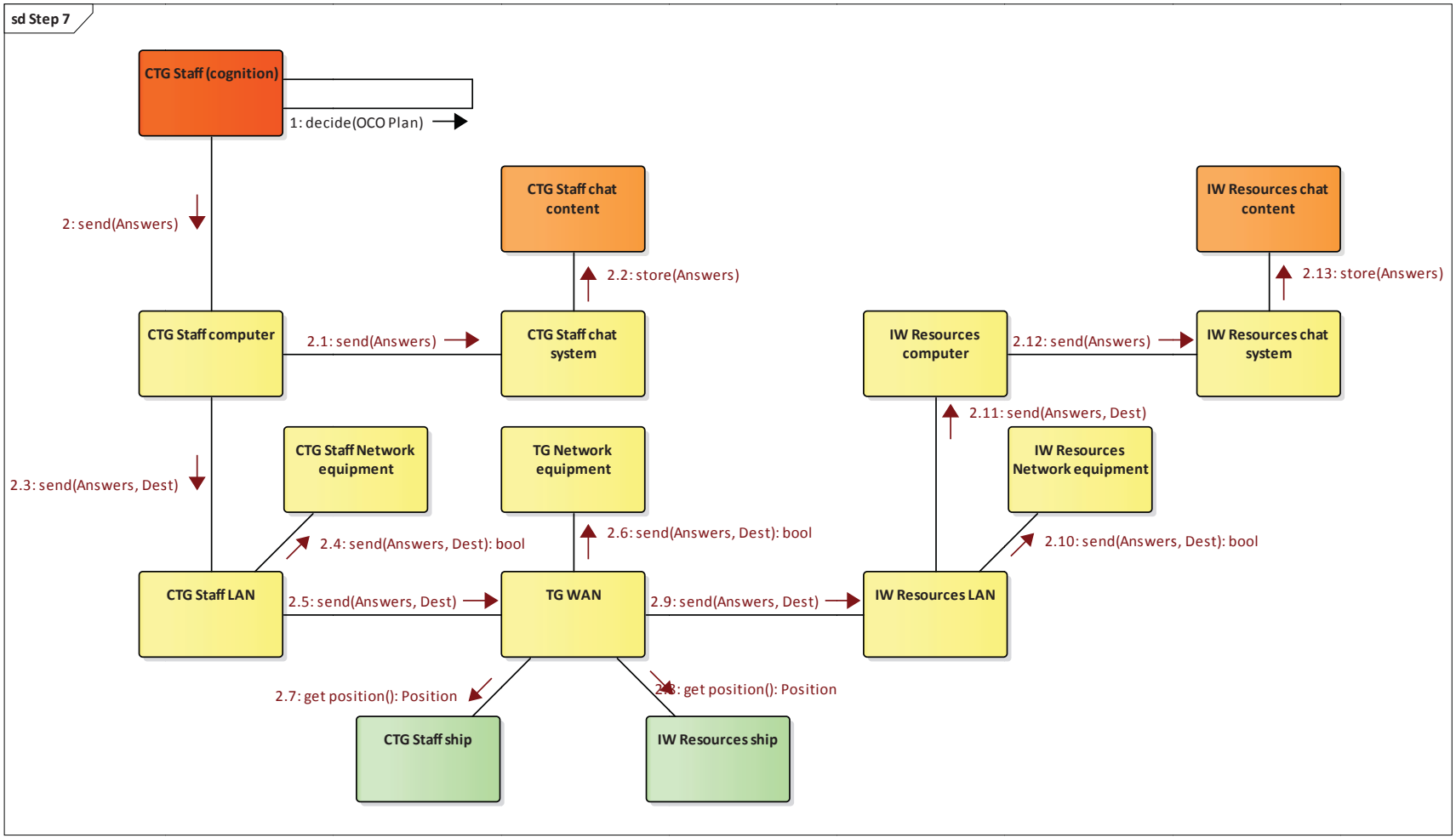

Figure 5-7: Communication Diagram for Step 7

CTG Staff Clarifies OCO Plan via Electronic Chat

5.1.1.8 Step 8

Consider Step 8 in the Present OCO Simulation use case: IW Resources decide to use Facebook, Twitter and Instagram, using different aliases, and to try spear-phishing based on HUMINT. Table 5-8 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, only the Cognition and Content layers are involved.

Table 5-8: Operational Systems and Activities in Step 8

IW Resources Decide to Use Facebook, Twitter and Instagram, Using Different Aliases, and to Try Spear-Phishing Based on HUMINT

Operation System and Activity	Type	Layer
IW Resources decide how to implement the *OCO plan*	Decision Information	Cognition Content

Figure 5-8 contains a representation of step 8 as a UML communication diagram.

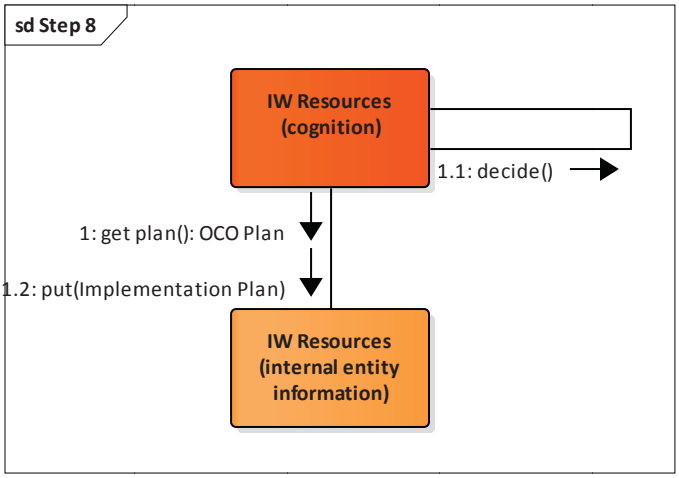

Figure 5-8: Communication Diagram for Step 8

IW Resources Decide to Use Facebook, Twitter and Instagram, Using Different Aliases, and to Try Spear-Phishing Based on HUMINT

5.1.1.9 Step 9

Consider Step 9 in the Present OCO Simulation use case: IW Resources post several messages to Facebook and Twitter using different aliases indicating the TG is in a particular area (that it is not). Table 5-9 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-9: Operational Systems and Activities in Step 9

IW Resources Post Several Messages to Facebook and Twitter Using Different Aliases Indicating TG is in a Particular Area (that it is not)

Operation System and Activity	Type	Layer
IW Resources uses	Action	Cognition
the *Facebook app*	Communication System	Conduit
to produce *Facebook content*	Information	Content
on the *IW Resources computer*,	Communication System	Conduit
which is then sent via the *IW Resources LAN*,	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
and the *Internet*	Communication System	Conduit
and takes *IW Resources ship* location into account,	Location	Physical
using the *Commercial Internet provider*,	Communication System	Conduit
to the *Facebook web service*	Communication System	Conduit
which stores each message as *Facebook content*	Information	Content
IW Resources uses	Action	Cognition
the *Twitter app*	Communication System	Conduit
to produce *Twitter content*	Information	Content
on the *IW Resources computer*,	Communication System	Conduit
which is then sent via the *IW Resources LAN*,	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
and the *Internet*	Communication System	Conduit
and takes *IW Resources ship* location into account,	Location	Physical
using the *Commercial Internet provider*,	Communication System	Conduit
to the *Twitter web service*	Communication System	Conduit
which stores each message as *Twitter content*	Information	Content

Figure 5-9 contains a representation of Step 9 as a UML communication diagram.

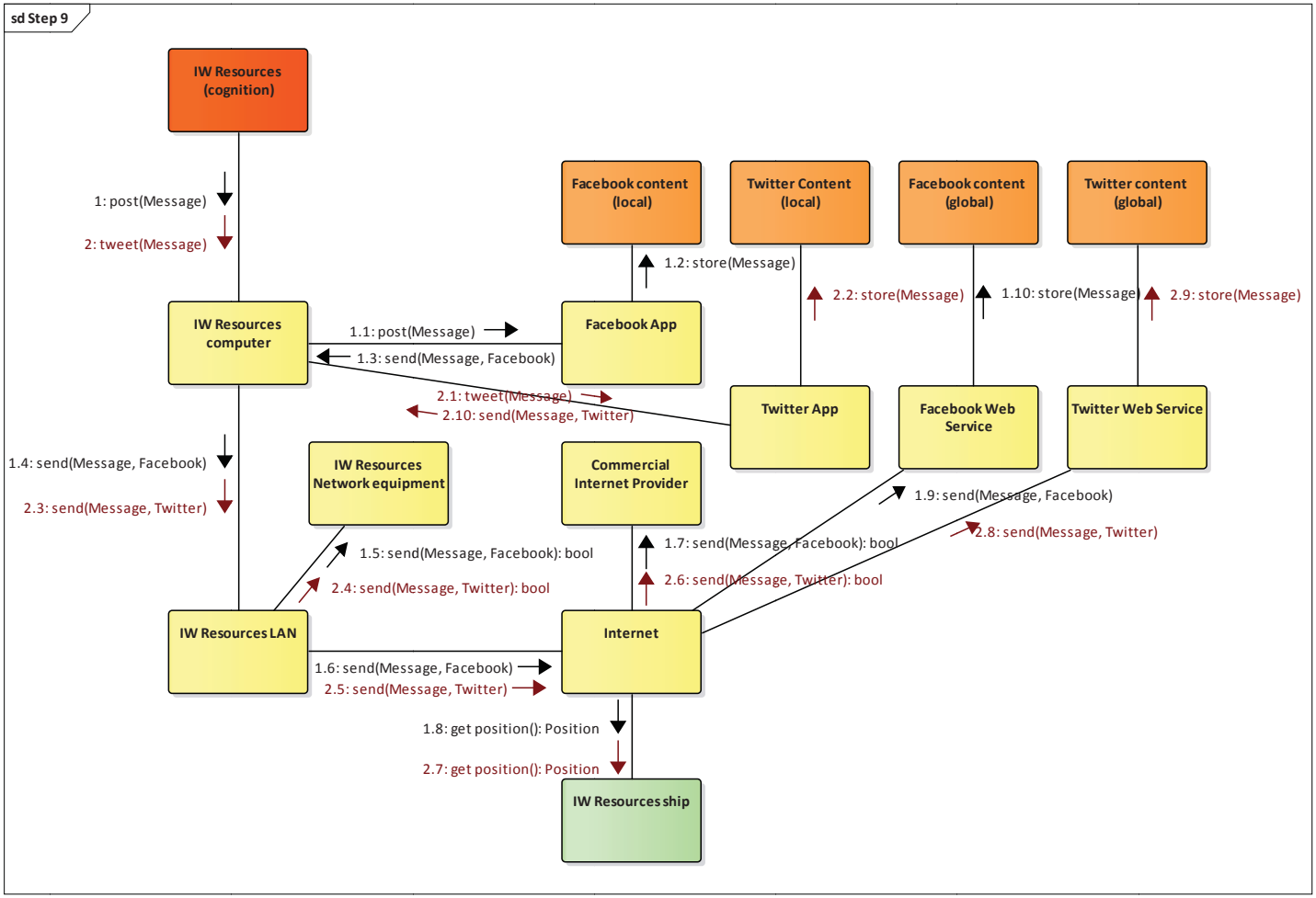

Figure 5-9: Communication Diagram for Step 9

IW Resources Post Several Messages to Facebook and Twitter Using Different Aliases Indicating TG is in a Particular Area (that it is Not)

5.1.1.10 Step 10

Consider Step 10 in the Present OCO Simulation use case: 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). Table 5-10 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-10: Operational Systems and Activities in Step 10

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)

Operation System and Activity	Type	Layer
IW Resources uses	Action	Cognition
the *Twitter app* to	Communication System	Conduit
produce *Twitter content* with incorrect geotags	Information	Content
on the *IW Resources cell phone*,	Communication System	Conduit
which is then sent via the *Cell phone network*	Communication System	Conduit
taking the *IW Resources cell phone* location into account	Location	Physical
and the *Internet*,	Communication System	Conduit
to the *Twitter web service*	Communication System	Conduit
which stores each message as *Twitter content*	Information	Content
IW Resources uses	Action	Cognition
the *Instagram app* to	Communication System	Conduit
produce *Instagram content* with incorrect geotags	Information	Content
on the *IW Resources cell phone*,	Communication System	Conduit
which is then sent via the *Cell phone network*	Communication System	Conduit
taking the *IW Resources cell phone* location into account	Location	Physical
and the *Internet*,	Communication System	Conduit
to the *Instagram web service*	Communication System	Conduit
which stores each message as *Instagram content*	Information	Content

Figure 5-10 contains a representation of step 10 as a UML communication diagram.

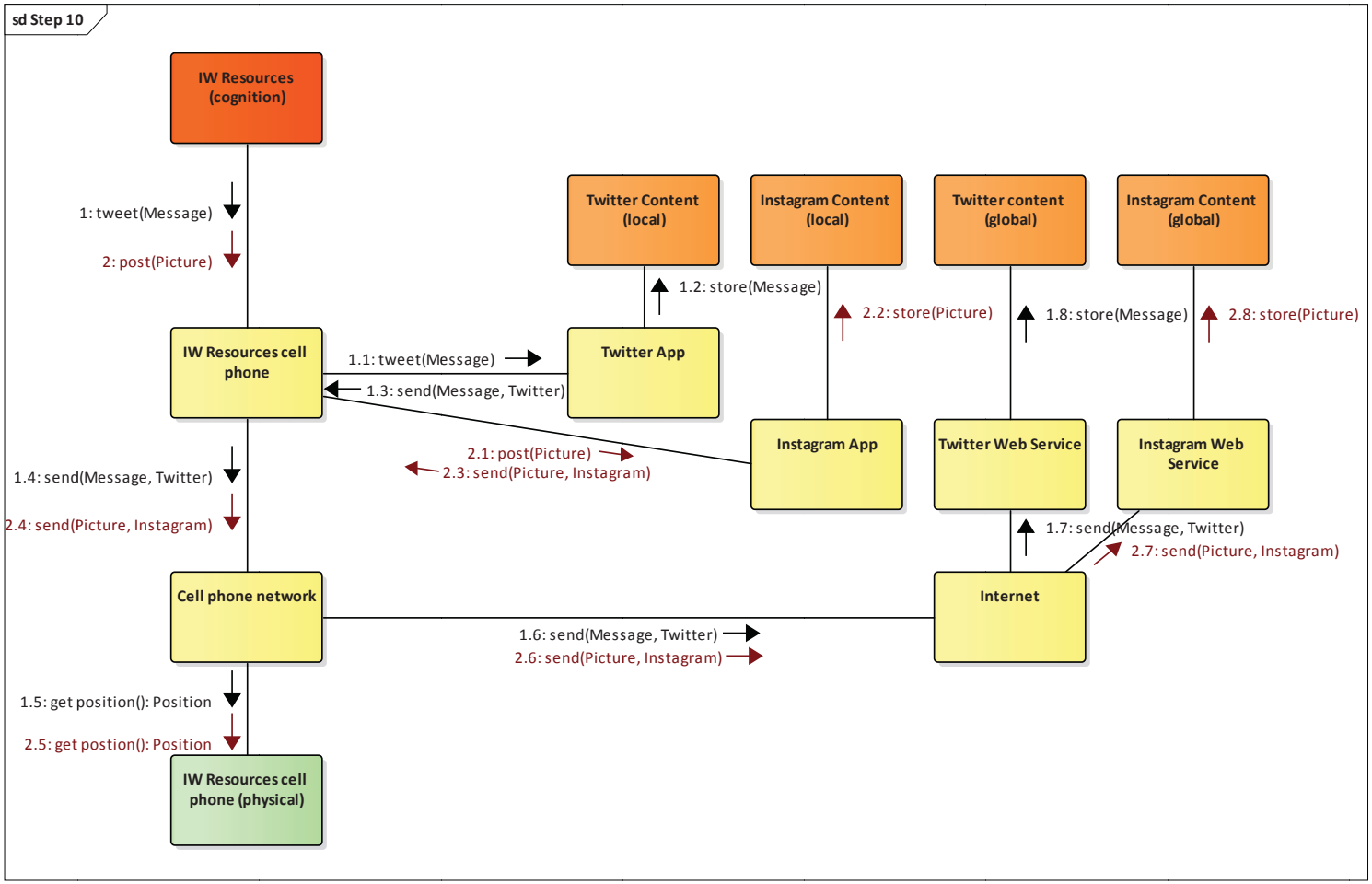

Figure 5-10: Communication Diagram for Step 10

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)

5.1.1.11 Step 11

Consider step 11 in the Present OCO Simulation use case: Adversary sees the messages and pictures and, taking their own opinions and cognitive biases into account, decides to stay away from the indicated area. Table 5-11 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-11: Operational Systems and Activities in Step 11

Adversary sees the messages and pictures and, taking their own opinions and cognitive biases into account, decides to stay away from the indicated area

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* to	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* to	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

Operation System and Activity	Type	Layer
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

Figure 5-11 contains a representation of step 11 as a UML communication diagram.

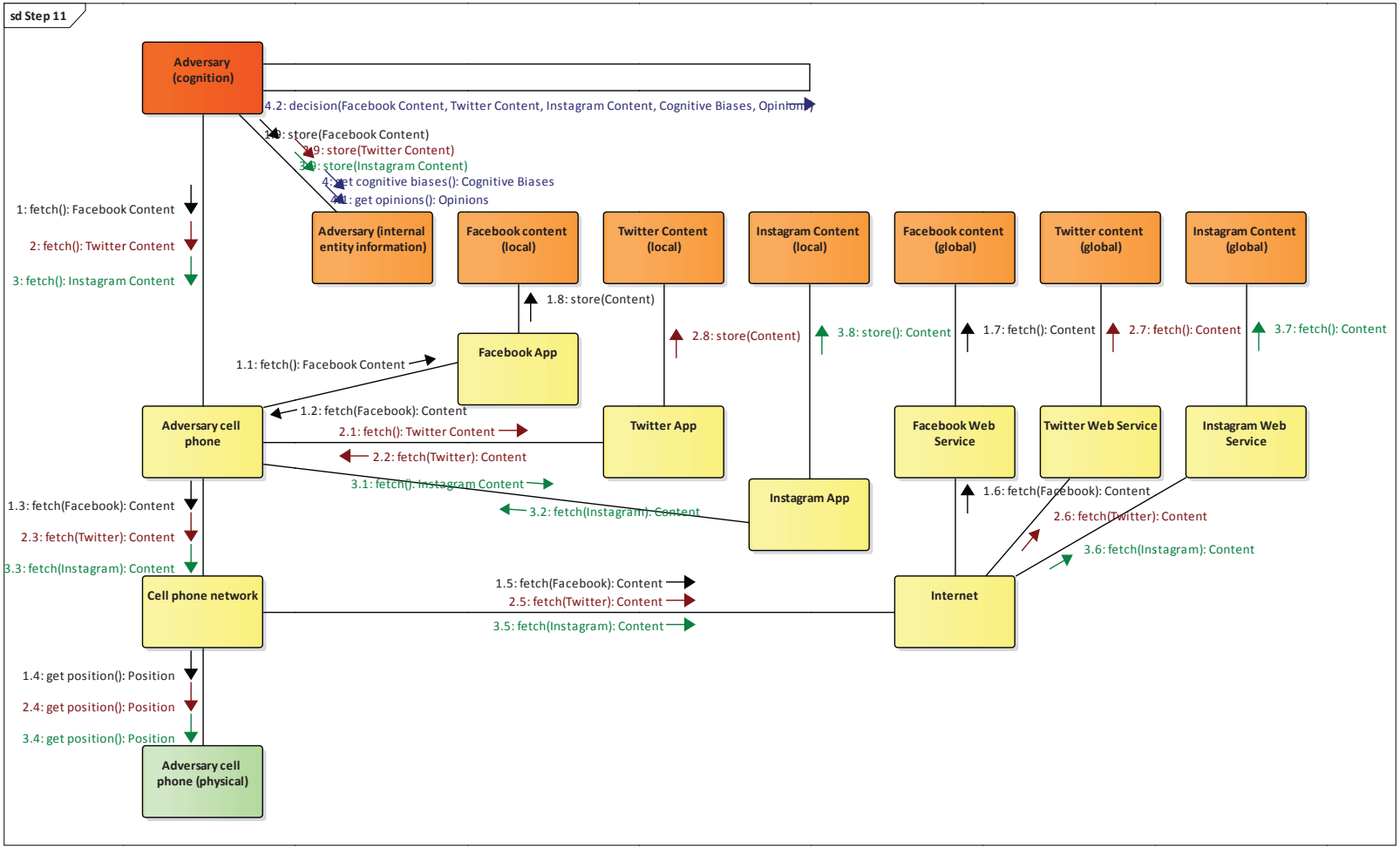

Figure 5-11: Communication Diagram for Step 11

Adversary sees the messages and pictures and, taking their own opinions and cognitive biases into account, decides to stay away from the indicated area

5.1.1.12 Step 12

Consider step 12 in the Present OCO Simulation use case: IW Resources prepare and send spear-phishing e-mail directed at the Adversary, and report to CTG Staff that e-mail has been sent. Table 5-12 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-12: Operational Systems and Activities in Step 12

IW Resources prepare and send spear-phishing e-mail directed at the Adversary, and report to CTG Staff that e-mail has been sent

Operation System and Activity	Type	Layer
IW Resources create spear-phishing e-mail	Action	Cognition
using *IW Resources computer*	Communication System	Conduit
and *IW Resources e-mail system*,	Communication System	Conduit
it is stored as *IW Resources e-mail content*	Information	Content
IW Resources sends created e-mail to addressee	Action	Cognition
using *IW Resources e-mail system*	Communication System	Conduit
on the *IW Resources computer*;	Communication System	Conduit
IW Resources e-mail system sends e-mail	Communication System	Conduit
from *IW Resources e-mail content*	Information	Content
routing it over *IW Resources LAN*	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
and the *Internet*	Communication System	Conduit
and takes *IW Resources ship* location	Location	Physical
and the *Adversary cell phone* location into account,	Location	Physical
and the *Adversary Wi-Fi LAN*	Communication System	Conduit
which uses *Adversary Network* equipment	Communication System	Conduit
to the *Adversary cell phone e-mail client*	Communication System	Conduit
on the *Adversary cell phone*,	Communication System	Conduit
the e-mail is stored as *Adversary e-mail content*	Information	Content
IW Resources create SITREP e-mail	Action	Cognition
using *IW Resources computer*	Communication System	Conduit
and *IW Resources e-mail system*,	Communication System	Conduit
it is stored as *IW Resources e-mail content*	Information	Content
IW Resources sends created e-mail to addressee	Action	Cognition
using *IW Resources e-mail system*	Communication System	Conduit
on the *IW Resources computer*;	Communication System	Conduit
IW Resources e-mail system sends e-mail	Communication System	Conduit

Operation System and Activity	Type	Layer
from *IW Resources e-mail content*	Information	Conduit
routing it over *IW Resources LAN*	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
TG WAN	Communication System	Conduit
which uses *TG Network* equipment	Communication System	Conduit
and takes *IW Resources ship* and *CTG Staff ship* locations into account,	Location	Physical
CTG Staff LAN	Communication System	Conduit
which uses *CTG Staff Network* equipment,	Communication System	Conduit
to the *CTG Staff e-mail system*	Communication System	Conduit
on the *CTG Staff computer*,	Communication System	Conduit
the e-mail is stored as *CTG Staff e-mail content*	Information	Content

Figure 5-12 contains a representation of step 12 as a UML communication diagram.

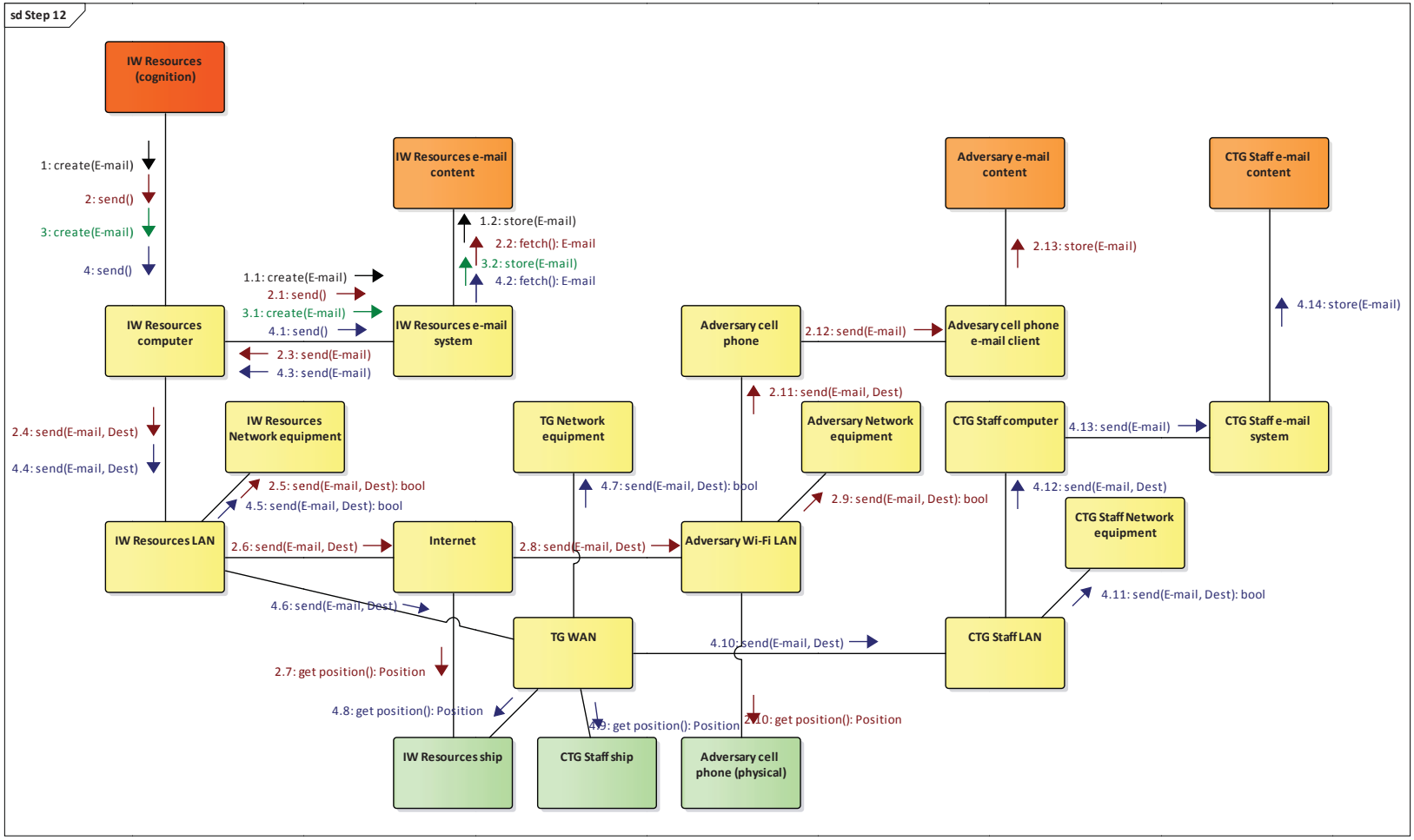

Figure 5-12: Communication Diagram for Step 12

IW Resources prepare and send spear-phishing e-mail directed at the Adversary, and report to CTG Staff that e-mail has been sent

5.1.1.13 Step 13

Consider step 13 in the Present OCO Simulation use case: 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 Website #1 containing malware. Table 5-13 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-13: Operational Systems and Activities in Step 13

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 Website #1 containing malware

Operation System and Activity	Type	Layer
Adversary opens	Action	Cognition
Adversary cell phone e-mail client	Communication System	Conduit
on the *Adversary cell phone*	Communication System	Conduit
and reads the spear-phishing e-mail stored as *Adversary e-mail content*	Information	Content
Adversary decides to click on the link in the e-mail	Decision	Cognition
Adversary clicks on spear-phishing link	Action	Cognition
through the *Adversary cell phone e-mail client*	Communication System	Conduit
on the *Adversary cell phone*	Communication System	Conduit
which opens *Adversary cell phone web browser*,	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 connect to *Website #1*	Communication System	Conduit
and download *Website content*,	Information	Content
including *Malware*	Information System	Content

Figure 5-13 contains a representation of step 13 as a UML communication diagram. It includes a note that during this step the malware is contained within the website content.

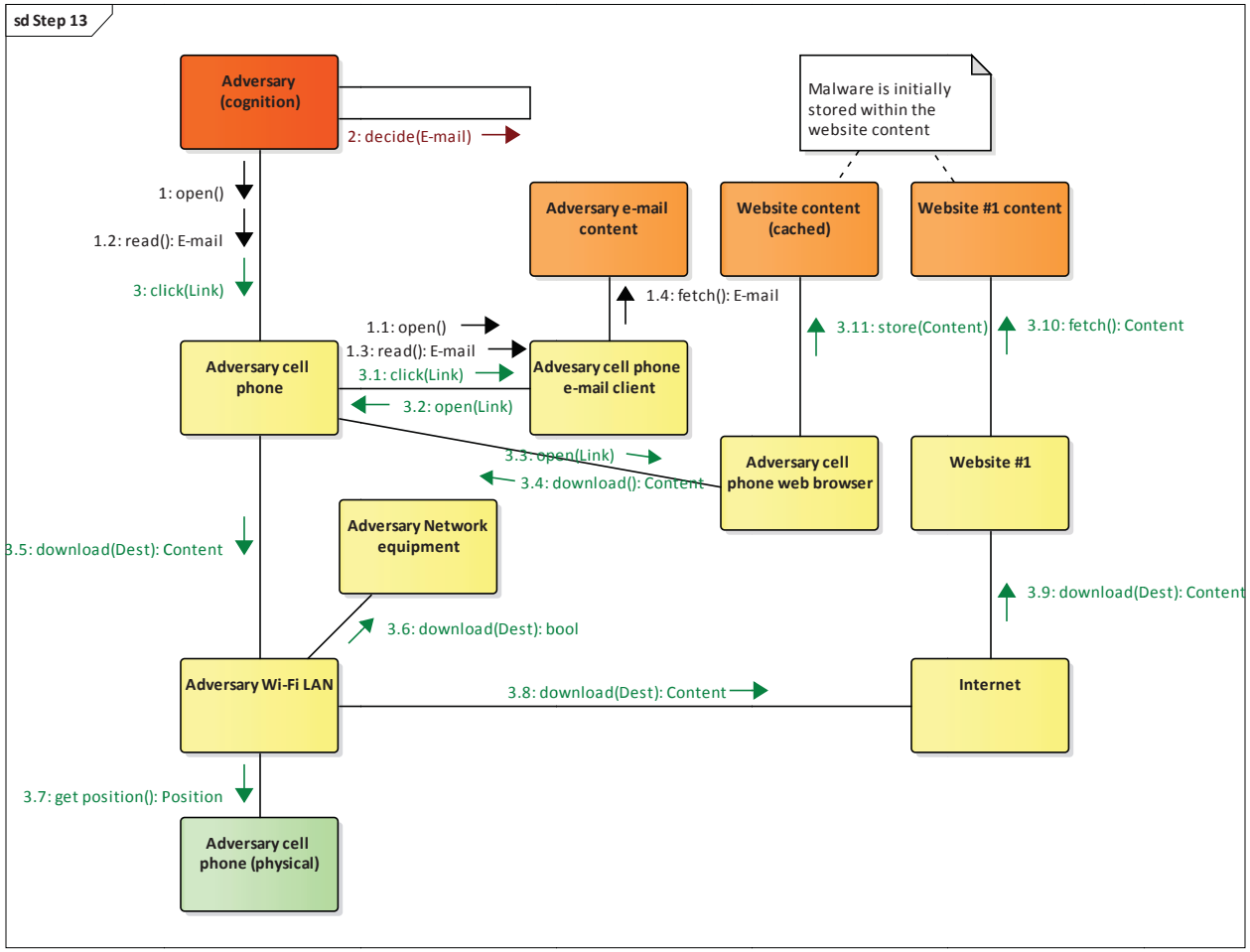

Figure 5-13: Communication Diagram for Step 13

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 Website #1 containing malware

5.1.1.14 Step 14

Consider step 14 in the Present OCO Simulation use case: Malware installs on the Adversary's cell phone, then connects to Website #2 and reports Adversary's position; Adversary's anti-virus software does not detect the presence or actions of the Malware. Table 5-14 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, the Content, Conduit and Physical layers in the IWSA are involved.

Table 5-14: Operational Systems and Activities in Step 14

Malware installs on the Adversary's cell phone, then connects to Website #2 and reports Adversary's position; Adversary's anti-virus software does not detect the presence or actions of the Malware

Operation System and Activity	Type	Layer
Malware exploits a bug	Information System	Content[3]
in the *Adversary cell phone web browser*	Communication System	Conduit
and installs on *Adversary cell phone*	Communication System	Conduit
Malware retrieves the position	Information System	Content
from the *Adversary cell phone*	Location	Physical
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 *Website #2*	Communication System	Conduit
and report the position	Information	Content
Anti-Virus Software	Information System	Content[4]
on the *Adversary cell phone*	Communication System	Conduit
do not trigger an alert	Information	Content

Figure 5-14 contains a representation of step 14 as a UML communication diagram. Note that the Malware sending data to Website #2 is represented by messages 3 and 3.x.

[3] As we discussed in Section 4.2.1.4, software that is sufficiently sophisticated to make complex decisions could be considered to be a part of the Cognition layer. For the purposes of this example, we do not consider the *Malware* to be that sophisticated.
[4] For the purposes of this example, we also do not consider the *Anti-Virus Software* to be sufficiently sophisticated to make decisions that we regard as complex, and so we do not consider it a part of the Cognition layer.

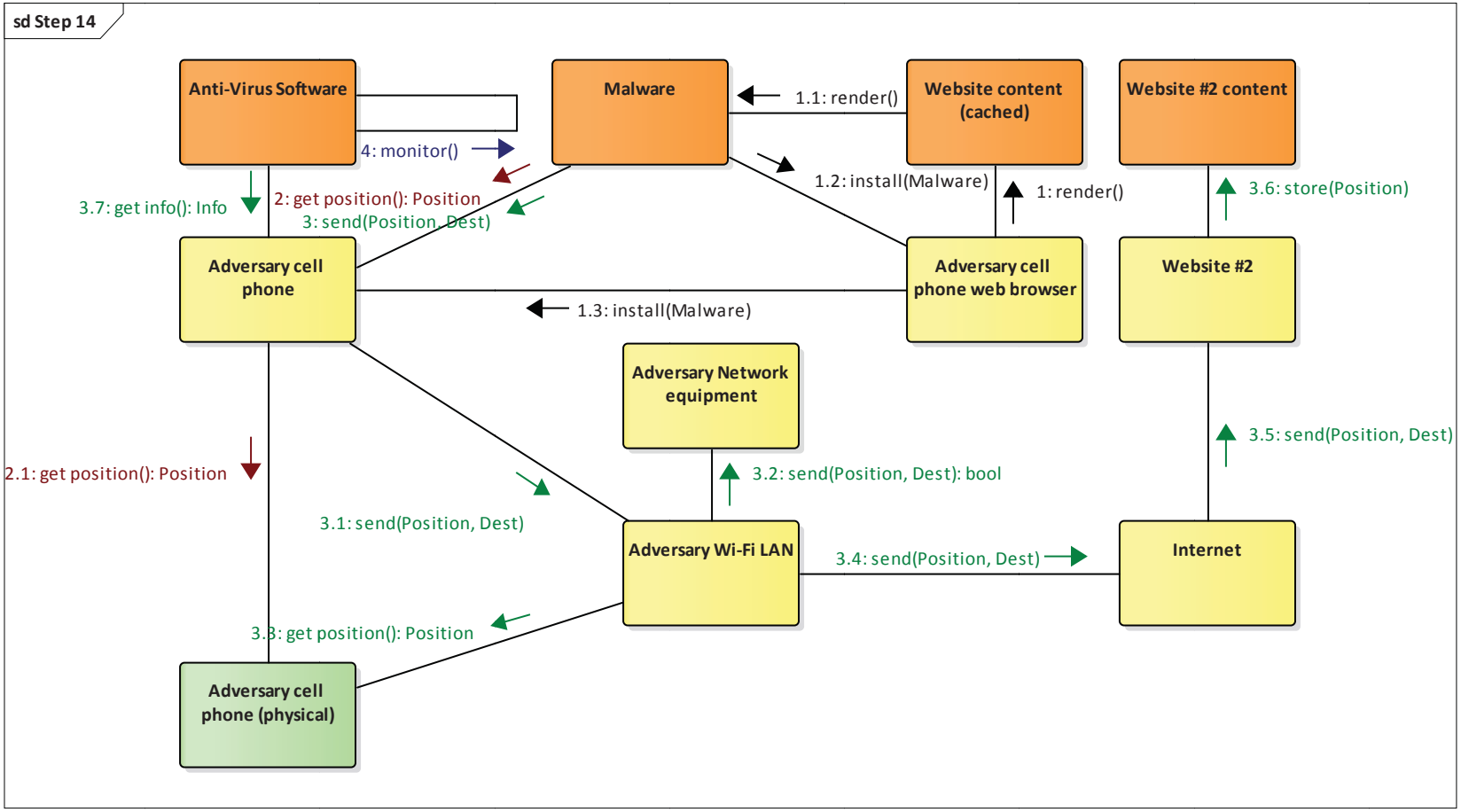

Figure 5-14: Communication Diagram for Step 14

Malware installs on the Adversary's cell phone, then connects to Website #2 and reports Adversary's position; Adversary's anti-virus software does not detect the presence or actions of the Malware

5.1.1.15 Step 15

Consider step 15 in the Present OCO Simulation use case: IW Resources check website #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. Table 5-15 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-15: Operational Systems and Activities in Step 15

IW Resources check Website #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

Operation System and Activity	Type	Layer
IW Resources uses	Action	Cognition
the *IW Resources web browser*	Communication System	Conduit
on the *IW Resources computer*,	Communication System	Conduit
via the *IW Resources LAN*,	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
and the *Internet*	Communication System	Conduit
and takes *IW Resources ship* location into account,	Location	Physical
using the *Commercial Internet provider*,	Communication System	Conduit
to *Website #2*	Communication System	Conduit
to retrieve *Website content*	Information	Content
containing the report from the *Malware*	Information	Content
IW Resources create SITREP e-mail	Action	Cognition
using *IW Resources computer*	Communication System	Conduit
and *IW Resources e-mail system*,	Communication System	Conduit
it is stored as *IW Resources e-mail content*	Information	Content
IW Resources sends created e-mail to addressee	Action	Cognition
using *IW Resources e-mail system*	Communication System	Conduit
on the *IW Resources computer*;	Communication System	Conduit
IW Resources e-mail system sends e-mail	Communication System	Conduit
from *IW Resources e-mail content*	Information	Content
routing it over *IW Resources LAN*	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
TG WAN	Communication System	Conduit
which uses *TG Network* equipment	Communication System	Conduit
and takes *IW Resources ship* and *CTG Staff ship* locations into account,	Location	Physical

Operation System and Activity	Type	Layer
CTG Staff LAN	Communication System	Conduit
which uses *CTG Staff Network* equipment,	Communication System	Conduit
to the *CTG Staff e-mail system*	Communication System	Conduit
on the *CTG Staff computer*,	Communication System	Conduit
the e-mail is stored as *CTG Staff e-mail content*	Information	Content

Figure 5-15 contains a representation of step 15 as a UML communication diagram.

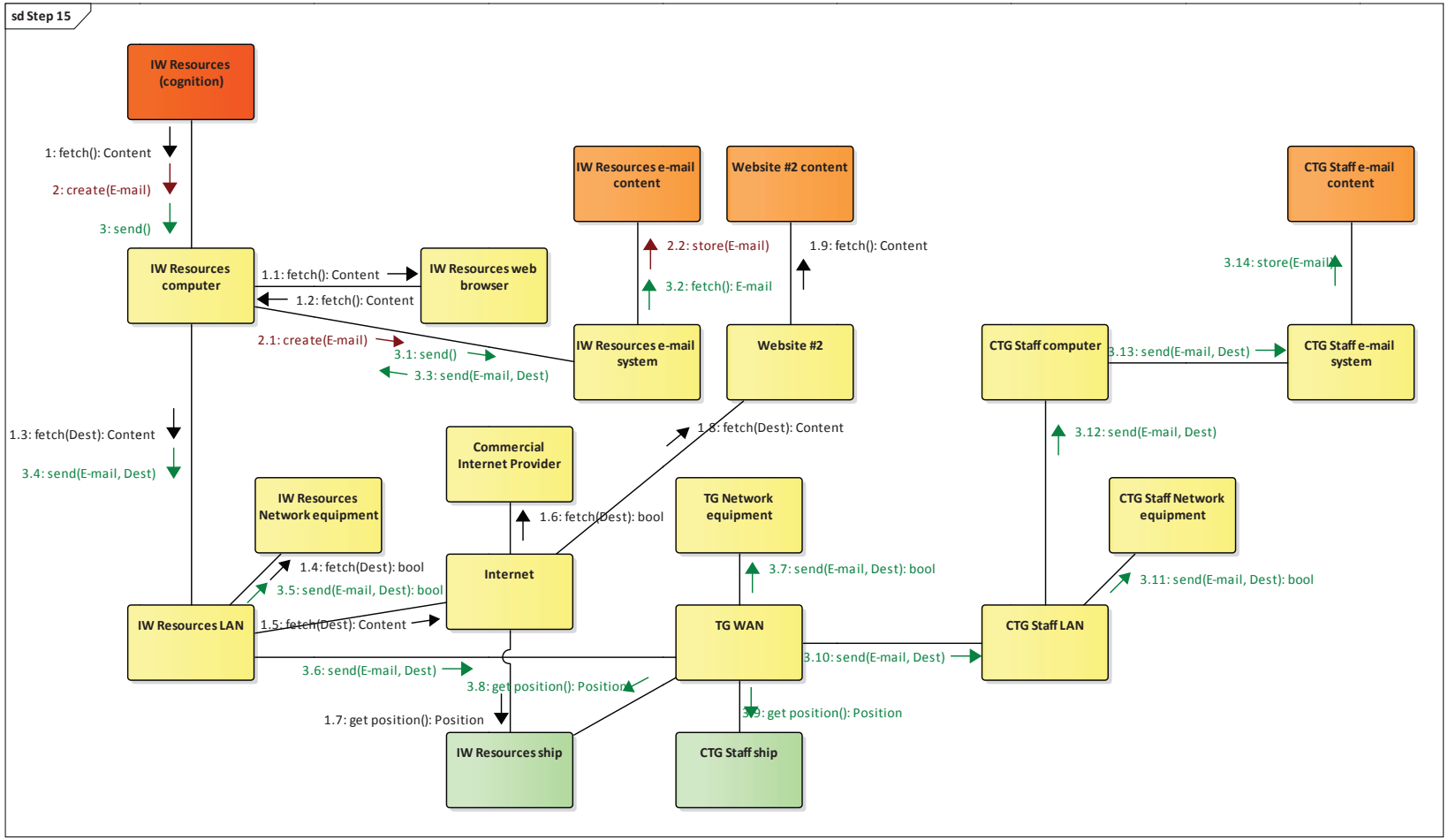

Figure 5-15: Communication Diagram for Step 15

IW Resources check Website #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

5.1.1.16 Step 16

Consider step 16 in the Present OCO Simulation use case: Adversary uses cell phone to plan human smuggling operation; Malware copies message data sent and received (SMS, e-mail, Signal) and voice recordings to Website #2. Table 5-16 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-16: Operational Systems and Activities in Step 16

Adversary uses cell phone to plan human smuggling operation; Malware copies message data sent and received (SMS, e-mail, Signal) and voice recordings to Website #2

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 *Website #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

Operation System and Activity	Type	Layer
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 *Website #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 *Website #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
remembering the messages sent	Information	Content
and interpreting and remembering messages received in the context of their cognitive biases	Information	Content
Malware	Information System	Content
on the *Adversary cell phone*	Communication System	Conduit

Operation System and Activity	Type	Layer
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 *Website #2*	Communication System	Conduit
and upload the voice recordings	Information	Content

Figure 5-16 contains a representation of step 16 as a UML communication diagram.

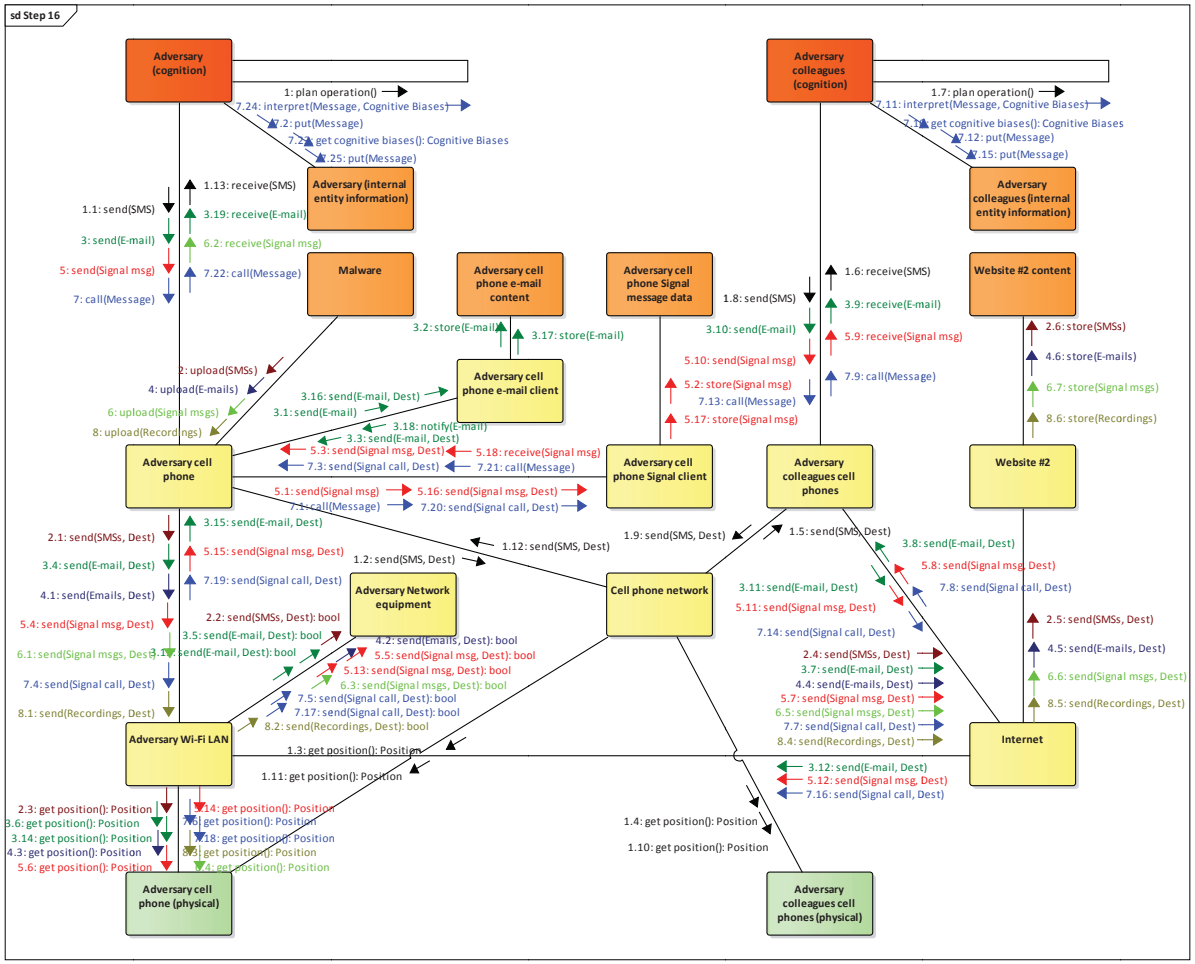

Figure 5-16: Communication Diagram for Step 16

Adversary uses cell phone to plan human smuggling operation; Malware copies message data sent and received (SMS, e-mail, Signal) and voice recordings to Website #2

5.1.1.17 Step 17

Consider step 17 in the Present OCO Simulation use case: IW Resources monitor Website #2 and reports plans of the Adversary to CTG Staff via e-mail. Table 5-17 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-17: Operational Systems and Activities in Step 17

IW Resources monitor Website #2 and reports plans of the Adversary to CTG Staff via e-mail

Operation System and Activity	Type	Layer
IW Resources uses	Action	Cognition
the *IW Resources web browser*	Communication System	Conduit
on the *IW Resources computer*,	Communication System	Conduit
via the *IW Resources LAN*,	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
and the *Internet*	Communication System	Conduit
and takes *IW Resources ship* location into account,	Location	Physical
using the *Commercial Internet provider*,		
to *Website #2*	Communication System	Conduit
to retrieve *Website content*	Communication System	Conduit
containing the message data and voice recordings	Information	Content
from the *Malware*	Information	Content
IW Resources uses	Action	Cognition
the *IW Resources computer*	Communication System	Conduit
to read the messages;	Information	Content
IW Resources uses	Action	Cognition
the *IW Resources computer*	Communication System	Conduit
to listen to the voice recordings	Information	Content
IW Resources interprets the messages and recordings	Observe	Cognition
IW Resources create SITREP e-mail	Action	Cognition
using *IW Resources computer*	Communication System	Conduit
and *IW Resources e-mail system*,	Communication System	Conduit
it is stored as *IW Resources e-mail content*	Information	Content
IW Resources sends created e-mail to addressee	Action	Cognition
using *IW Resources e-mail system*	Communication System	Conduit
on the *IW Resources computer*;	Communication System	Conduit
IW Resources e-mail system sends e-mail	Communication System	Conduit
from *IW Resources e-mail content*	Information	Content

Operation System and Activity	Type	Layer
routing it over *IW Resources LAN*	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
TG WAN	Communication System	Conduit
which uses *TG Network* equipment	Communication System	Conduit
and takes *IW Resources ship* and *CTG Staff ship* locations into account,	Location	Physical
CTG Staff LAN	Communication System	Conduit
which uses *CTG Staff Network* equipment,	Communication System	Conduit
to the *CTG Staff e-mail system*	Communication System	Conduit
on the *CTG Staff computer*,	Communication System	Conduit
the e-mail is stored as *CTG Staff e-mail content*	Information	Content

Figure 5-17 contains a representation of step 17 as a UML communication diagram.

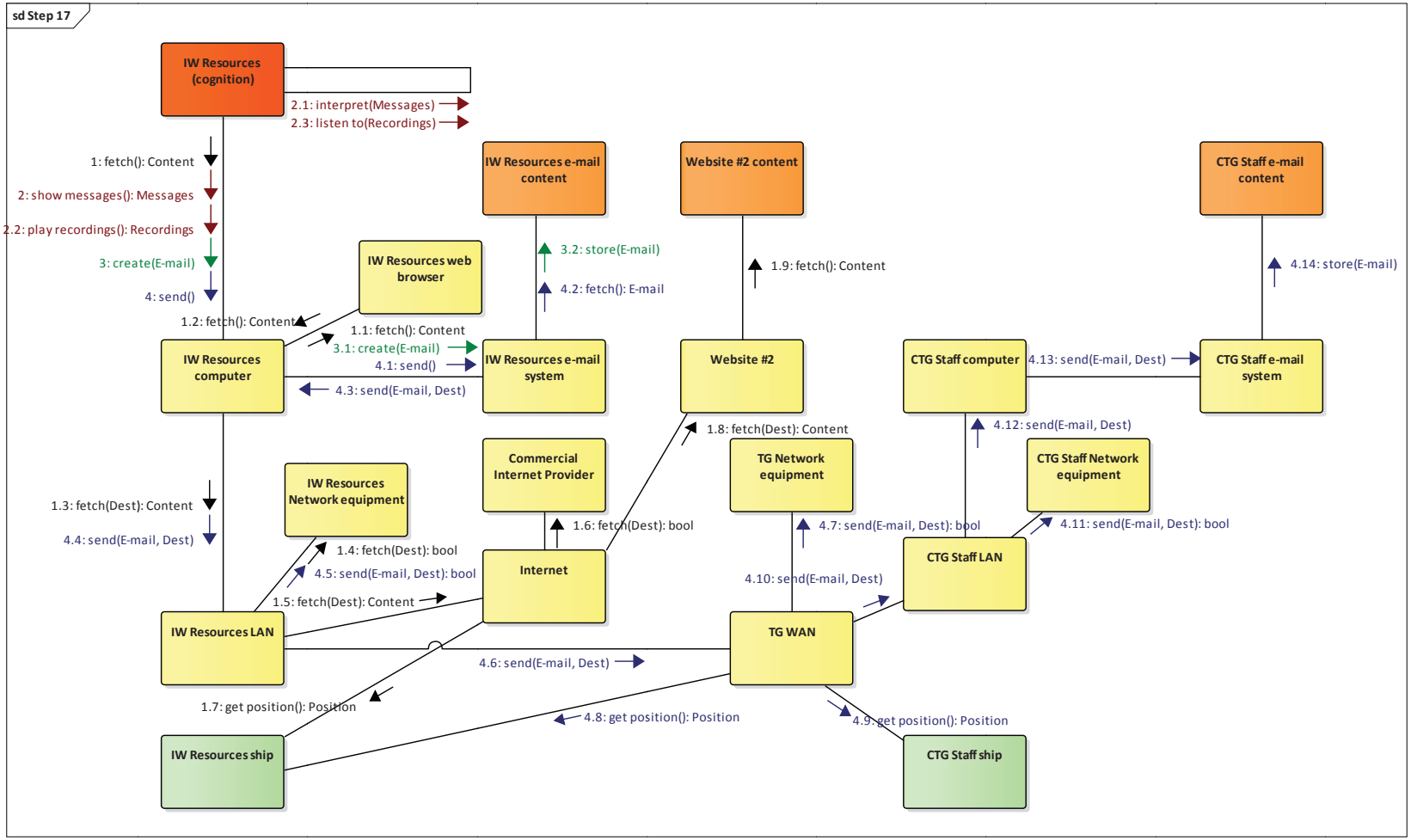

Figure 5-17: Communication Diagram for Step 17

IW Resources monitor Website #2 and reports plans of the Adversary to CTG Staff via e-mail

5.1.1.18 Step 18

Consider step 18 in the Present OCO Simulation use case: Adversary departs port on a human smuggling operation; Malware connects to Website #2 and reports Adversary's position. Table 5-18 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-18: Operational Systems and Activities in Step 18

Adversary departs port on a human smuggling operation; Malware connects to Website #2 and reports Adversary's position

Operation System and Activity	Type	Layer
Adversary decides to depart port	Decide	Cognition
Adversary boards *VOI*	Movement Location	Physical Physical
Adversary sails *VOI* and navigates out of port	Action Movement	Cognition Physical
Malware on the *Adversary cell phone* uses the *Cell phone network* which takes the *Adversary cell phone* location into account and the *Internet*, to connect to *Website #2* and report the position	Information System Communication System Communication System Location Communication System Communication System Information	Content Conduit Conduit Physical Conduit Conduit Content

Figure 5-18 contains a representation of step 18 as a UML communication diagram.

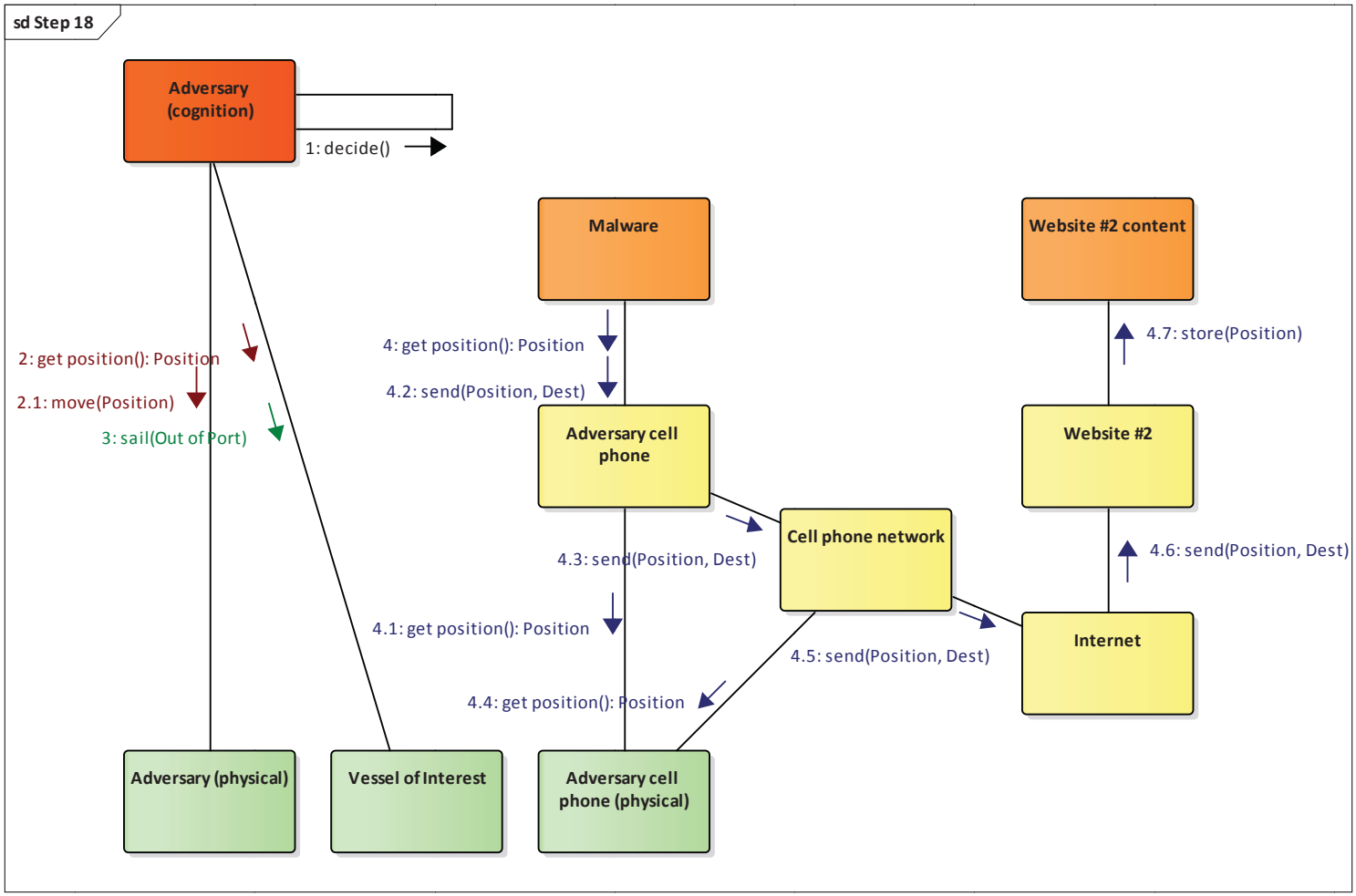

Figure 5-18: Communication Diagram for Step 18

Adversary departs port on a human smuggling operation; Malware connects to Website #2 and reports Adversary's position

5.1.1.19 Step 19

Consider step 19 in the Present OCO Simulation use case: IW Resources monitor Website #2 and report departure of the Adversary to CTG Staff via e-mail. Table 5-19 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-19: Operational Systems and Activities in Step 19

IW Resources monitor Website #2 and report departure of the Adversary to CTG Staff via e-mail

Operation System and Activity	Type	Layer
IW Resources uses	Action	Cognition
the *IW Resources web browser*	Communication System	Conduit
on the *IW Resources computer*,	Communication System	Conduit
via the *IW Resources LAN*,	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
and the *Internet*	Communication System	Conduit
and takes *IW Resources ship* location into account,	Location	Physical
using the *Commercial Internet provider*,	Communication System	Conduit
to *Website #2*	Communication System	Conduit
to retrieve *Website content*	Information	Content
containing the report from the *Malware*	Information	Content
IW Resources create SITREP e-mail	Action	Cognition
using *IW Resources computer*	Communication System	Conduit
and *IW Resources e-mail system*,	Communication System	Conduit
it is stored as *IW Resources e-mail content*	Information	Content
IW Resources sends created e-mail to addressee	Action	Cognition
using *IW Resources e-mail system*	Communication System	Conduit
on the *IW Resources computer*;	Communication System	Conduit
IW Resources e-mail system sends e-mail	Communication System	Conduit
from *IW Resources e-mail content*	Information	Content
routing it over *IW Resources LAN*	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
TG WAN	Communication System	Conduit
which uses *TG Network* equipment	Communication System	Conduit
and takes *IW Resources ship* and *CTG Staff ship* locations into account,	Location	Physical
CTG Staff LAN	Communication System	Conduit
which uses *CTG Staff Network* equipment,	Communication System	Conduit
to the *CTG Staff e-mail system*	Communication System	Conduit

Operation System and Activity	Type	Layer
on the *CTG Staff computer*, the e-mail is stored as *CTG Staff e-mail content*	Communication System Information	Conduit Content

Figure 5-19 contains a representation of step 19 as a UML communication diagram.

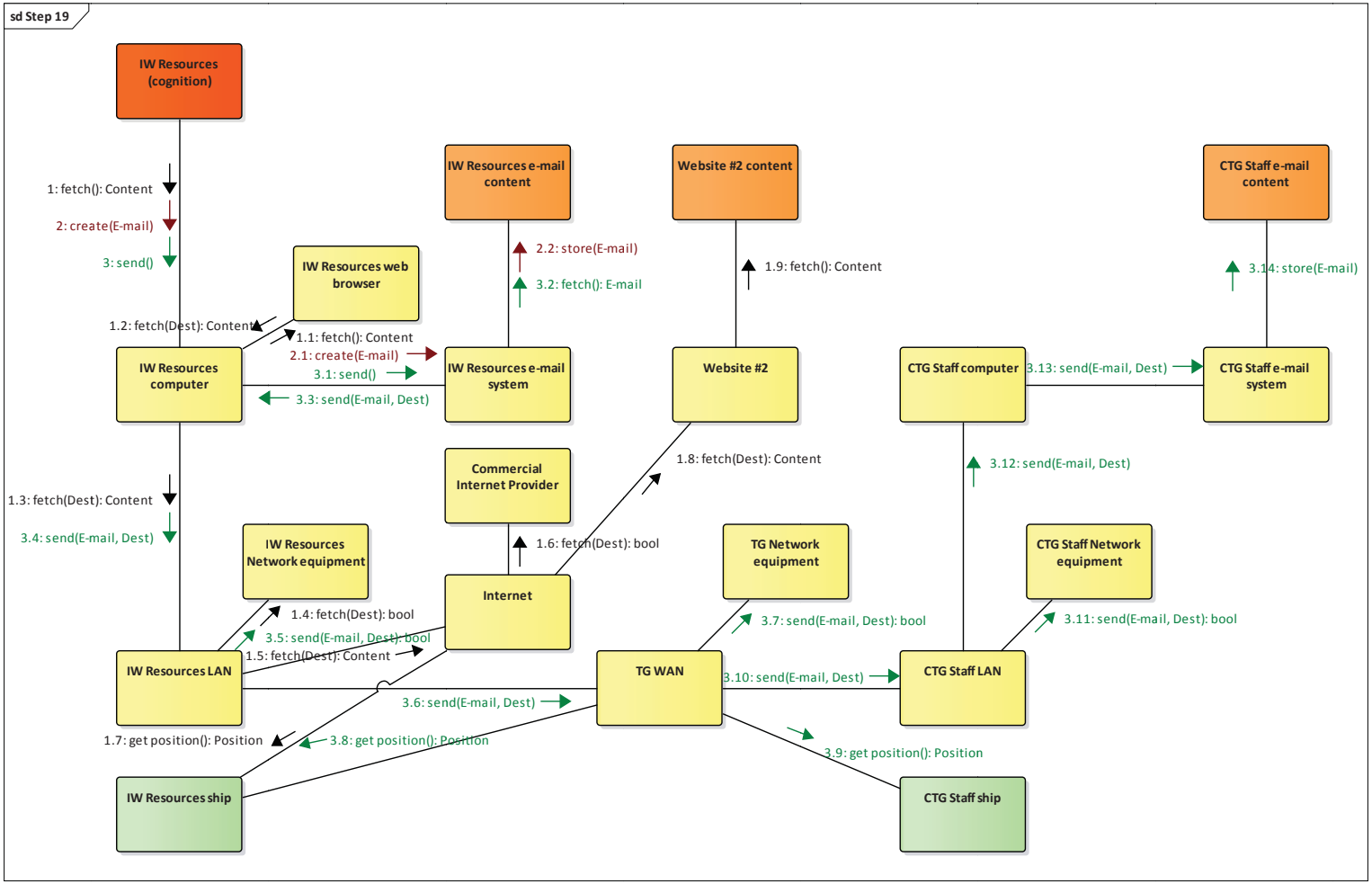

Figure 5-19: Communication Diagram for Step 19

IW Resources monitor Website #2 and report departure of the Adversary to CTG Staff via e-mail

5.1.1.20 Step 20

Consider step 20 in the Present OCO Simulation use case: CTG Staff orders TG to sail to intercept Adversary. Table 5-20 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, the Cognition and Physical layers in the IWSA are involved. The Conduit and Content layers (e.g., communication of the order to the IW Resources and EW Resources ships) have been omitted for clarity.

Table 5-20: Operational Systems and Activities in Step 20

CTG Staff orders TG to sail to intercept Adversary

Operation System and Activity	Type	Layer
CTG Staff orders TG to sail to intercept Adversary	Action (Command)	Cognition
TG ships navigate to intercept Adversary	Movement	Physical

Figure 5-20 contains a representation of step 20 as a UML communication diagram. Note that the result of omitting the Conduit and Content layer activities in this step result in a representation that is a lower fidelity than the communication and cyber elements in the earlier steps.

Figure 5-21 contains an enhanced representation of step 20 as a UML communication diagram that does include Conduit and Content layer activities, which demonstrates the additional complexity of modelling the additional components.

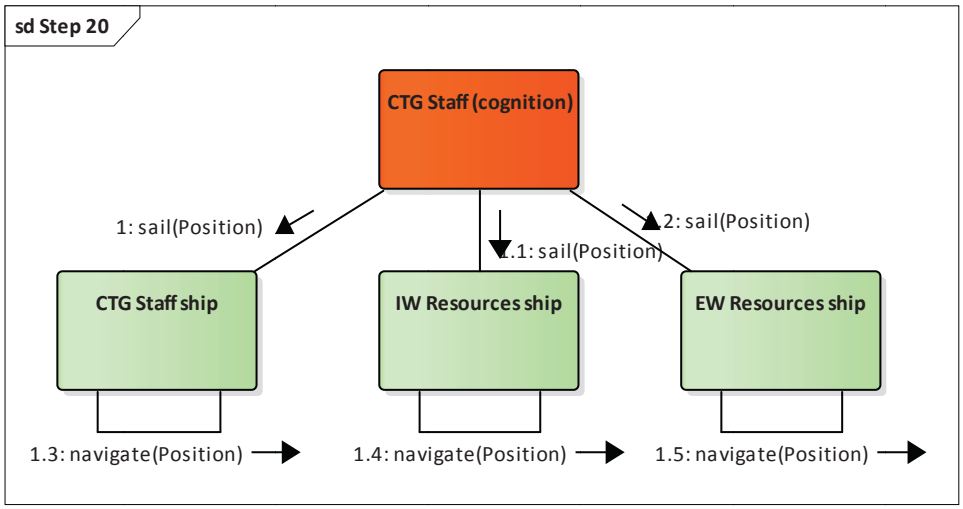

Figure 5-20: Communication Diagram for Step 20

CTG Staff orders TG to sail to intercept Adversary

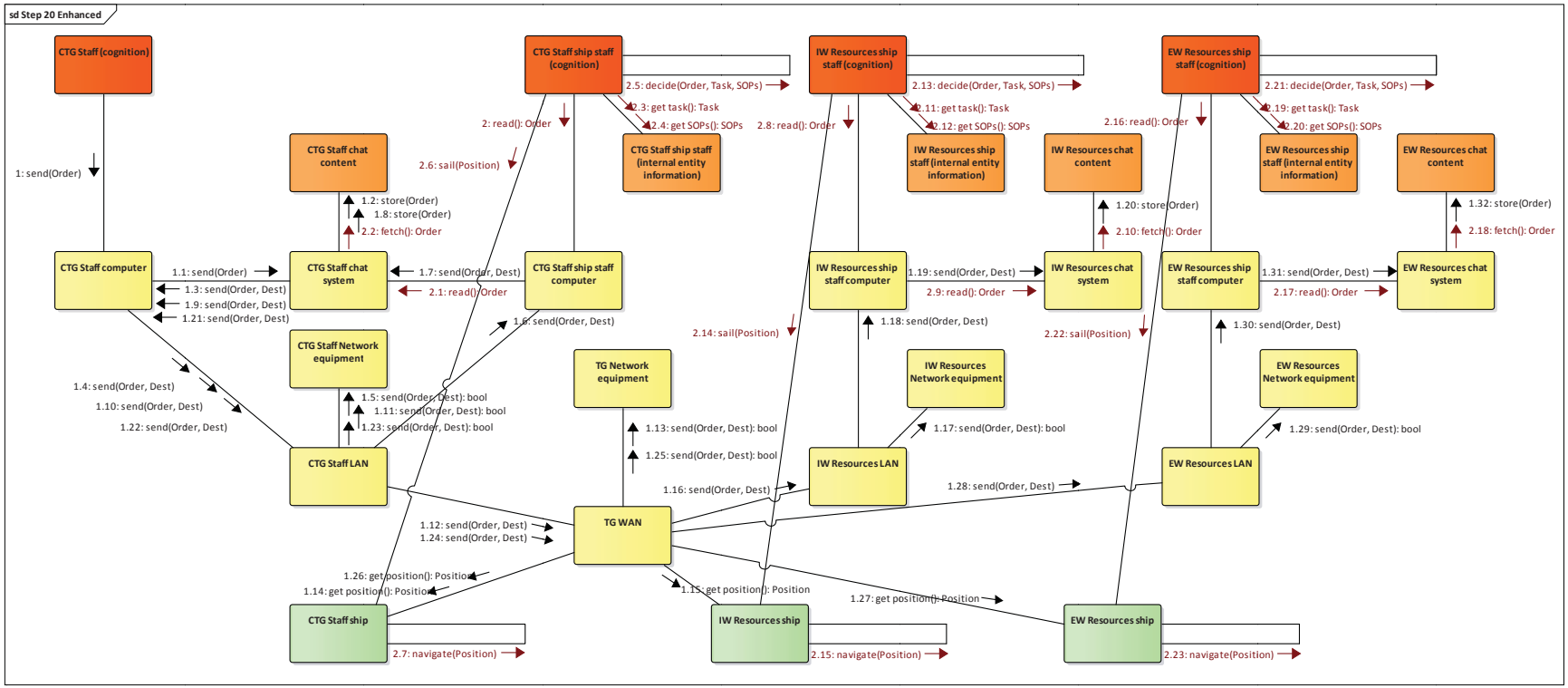

Figure 5-21: Enhanced Communication Diagram for Step 20

CTG Staff orders TG to sail to intercept Adversary

5.1.1.21 Step 21

Consider step 21 in the Present OCO Simulation use case: IW Resources command Malware to disable Adversary cell phone; Malware disables Adversary cell phone. Table 5-21 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-21: Operational Systems and Activities in Step 21

IW Resources command Malware to disable Adversary cell phone; Malware disables Adversary cell phone

Operation System and Activity	Type	Layer
IW Resources sends a command	Action (Command)	Cognition
using the *IW Resources computer*	Communication System	Conduit
via *IW Resources LAN*,	Communication System	Conduit
which uses *IW Resources Network* equipment,	Communication System	Conduit
and the *Internet*,	Communication System	Conduit
using the *Commercial Internet provider*	Communication System	Conduit
taking *IW Resources ship* location into account,	Location	Physical
and the *Cell phone network*	Communication System	Conduit
which takes the *Adversary cell phone* location into account	Location	Physical
to the *Malware*	Information System	Content
on the *Adversary cell phone*	Communication System	Conduit
Malware	Information System	Content
disables the *Adversary cell phone*	Communication System	Conduit

Figure 5-22 contains a representation of step 21 as a UML communication diagram.

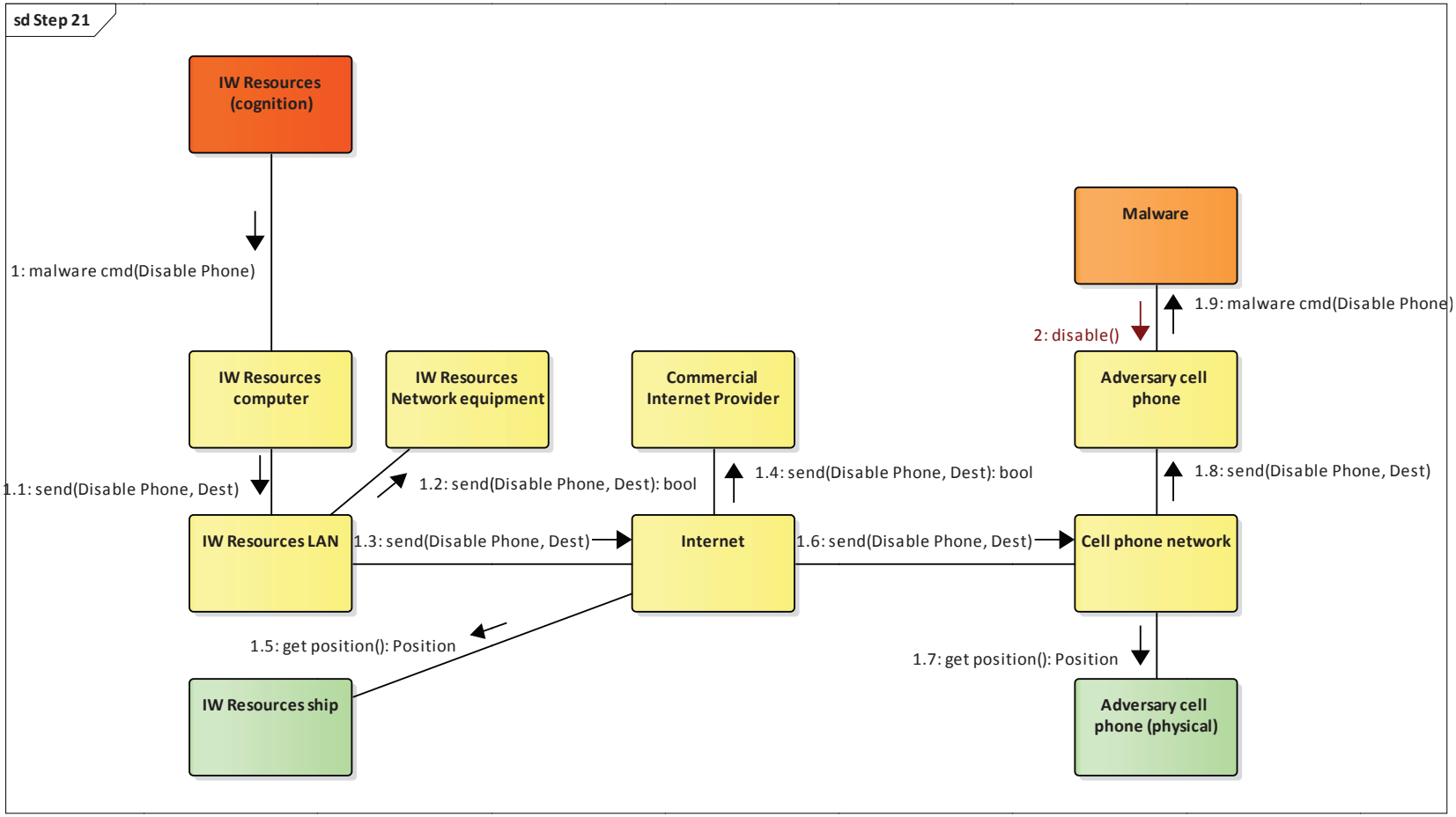

Figure 5-22: Communication Diagram for Step 21

IW Resources command Malware to disable Adversary cell phone; Malware disables Adversary cell phone

5.1.1.22 Step 22

Consider step 22 in the Present OCO Simulation use case: colleagues of Adversary attempt, but are unable, to call Adversary via cell phone. Table 5-22 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, the Cognition, Conduit and Physical layers in the IWSA are involved. This step demonstrates an error occurring, in contrast to all the previous steps in which success of each operation is assumed and not represented explicitly.

Table 5-22: Operational Systems and Activities in Step 22

Colleagues of Adversary attempt, but are unable, to call Adversary via cell phone

Operation System and Activity	Type	Layer
Adversary colleagues	Action	Cognition
uses *Adversary colleagues cell phones*	Communication System	Conduit
which uses the *Cell phone network,*	Communication System	Conduit
which takes the *Adversary colleagues cell phones* location into account,	Location	Physical
to try to call the *Adversary cell phone*	Communication System	Conduit
Cell phone network	Communication System	Conduit
fails to contact the *Adversary cell phone*	Communication System	Conduit
and returns an error	Information	Content

Figure 5-23 contains a representation of step 22 as a UML communication diagram.

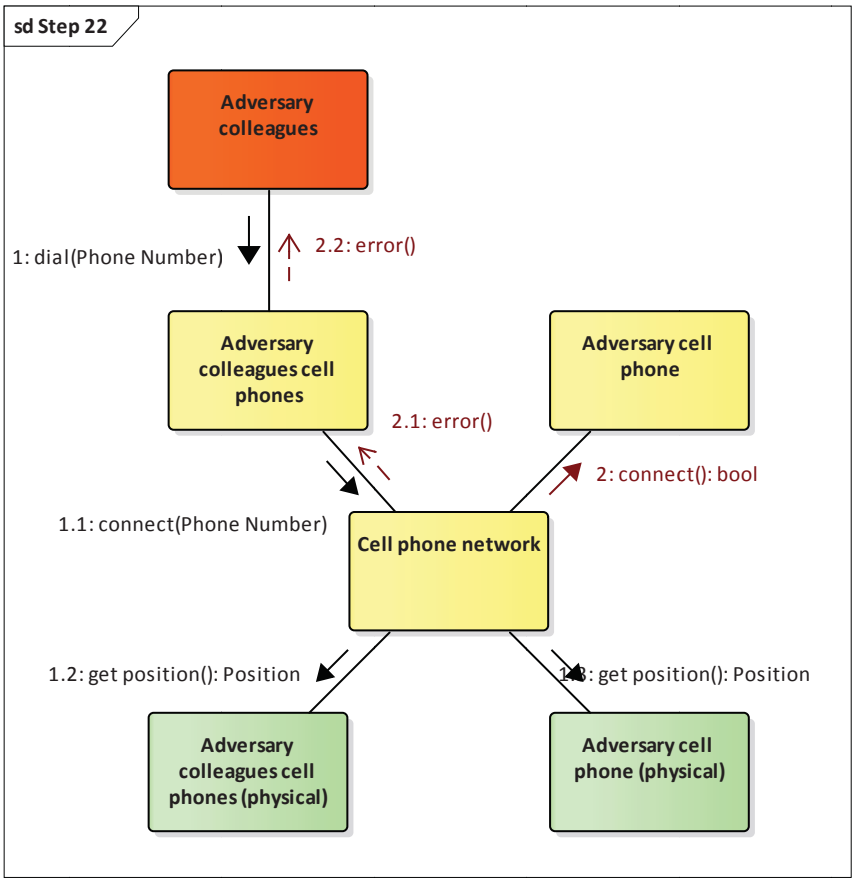

Figure 5-23: Communication Diagram for Step 22

Colleagues of Adversary attempt, but are unable, to call Adversary via cell phone

5.1.1.23 Step 23

Consider step 23 in the Present OCO Simulation use case: EW Resources monitor marine radio (COMINT) and hear a local fisherman discussing the TG; Adversary also hears and enters discussion. Table 5-23 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-23: Operational Systems and Activities in Step 23

EW Resources monitor marine radio (COMINT) and hear a local fisherman discussing the TG; Adversary also hears and enters discussion

Operation System and Activity	Type	Layer
Fisherman talks (remembering the message)	Action (speak) Information	Cognition Content

Operation System and Activity	Type	Layer
on *Marine Radio equipment* to transmit	Communication System	Conduit
on the *Marine Radio frequencies,*	Communication System	Conduit
whose reception is impacted by the *Fisherman boat* and *EW Resources ship* locations	Location	Physical
and is received by *COMINT sensor*	Communication System	Conduit
and heard by *EW Resources*	Action (listen)	Cognition
who interprets and remembers the messages heard in the context of their cognitive biases	Information	Content
and is recorded,	Information	Content
and impacted by the *Fisherman boat* and *EW Resources ship* locations	Location	Physical
and is received by *Marine Radio equipment*	Communication System	Conduit
and heard by *Adversary*	Action (listen)	Cognition
who interprets and remembers the messages heard in the context of their cognitive biases	Information	Content
Adversary responds	Action (speak)	Cognition
(remembering the message)	Information	Content
on *Marine Radio equipment* to transmit	Communication System	Conduit
on the *Marine Radio frequencies,*	Communication System	Conduit
whose reception is impacted by the *VOI* and *EW Resources ship* locations	Location	Physical
and is received by *COMINT sensor*	Communication System	Conduit
and heard by *EW Resources*	Action (listen)	Cognition
who interprets and remembers the messages heard in the context of their cognitive biases	Information	Content
and recorded,	Information	Content
and impacted by the *VOI* and *Fisherman boat* locations	Location	Physical
and is received by *Marine Radio equipment*	Communication System	Conduit
and heard by *Fisherman*	Action (listen)	Cognition
who interprets and remembers the messages heard in the context of their cognitive biases	Information	Content

Figure 5-24 contains a representation of step 23 as a UML communication diagram.

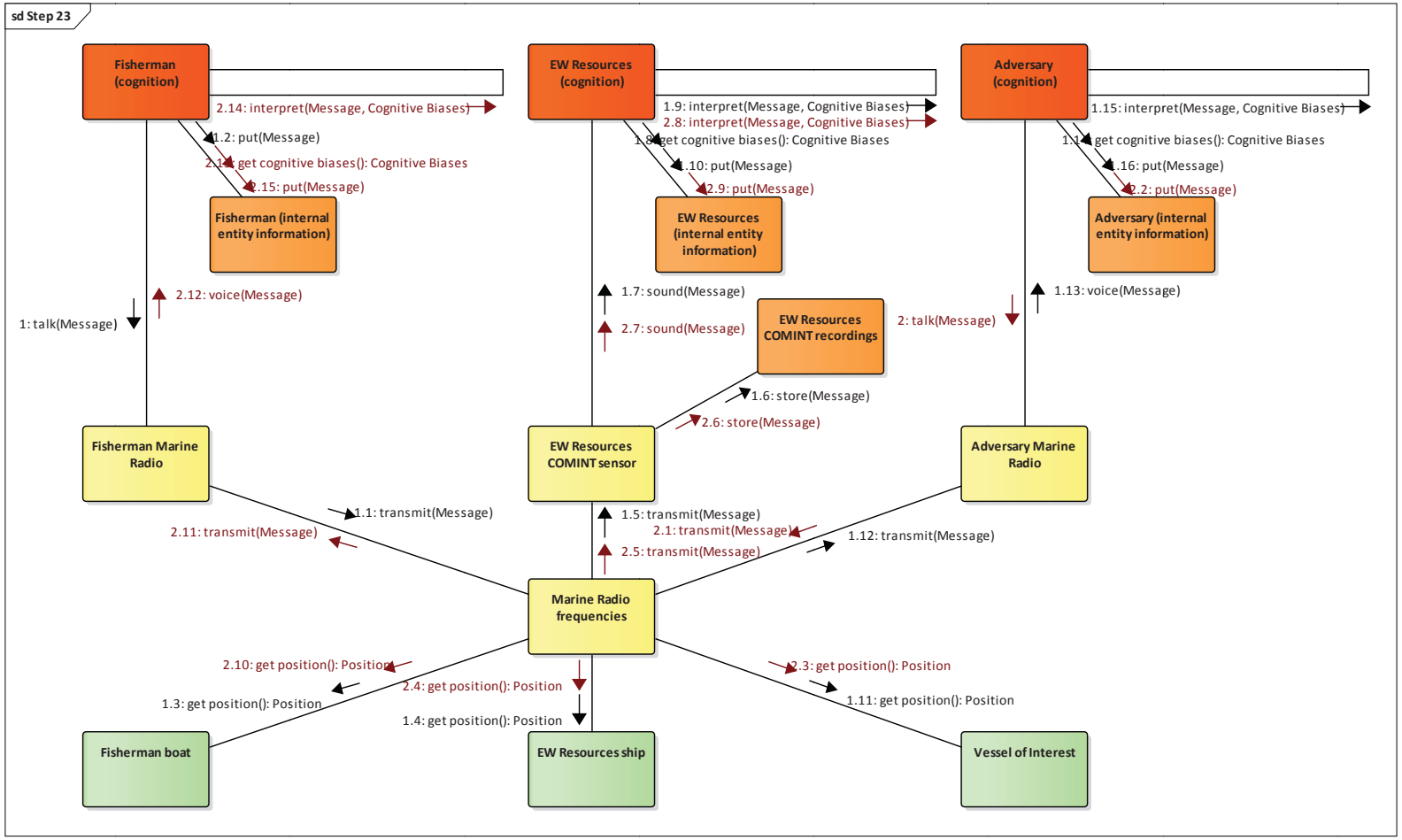

Figure 5-24: Communication Diagram for Step 23

EW Resources monitor marine radio (COMINT) and hear a local fisherman discussing the TG; Adversary also hears and enters discussion

5.1.1.24 Step 24

Consider step 24 in the Present OCO Simulation use case: Adversary changes course based on the discussion. Table 5-24 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, the Cognition, Content and Physical layers in the IWSA are involved.

Table 5-24: Operational Systems and Activities in Step 24

Adversary changes course based on the discussion

Operation System and Activity	Type	Layer
Adversary decides to change course in the context of their opinions and cognitive biases	Decision Information	Cognition Content
Adversary changes the course of the *VOI*	Action Movement	Cognition Physical

Figure 5-25 contains a representation of step 24 as a UML communication diagram.

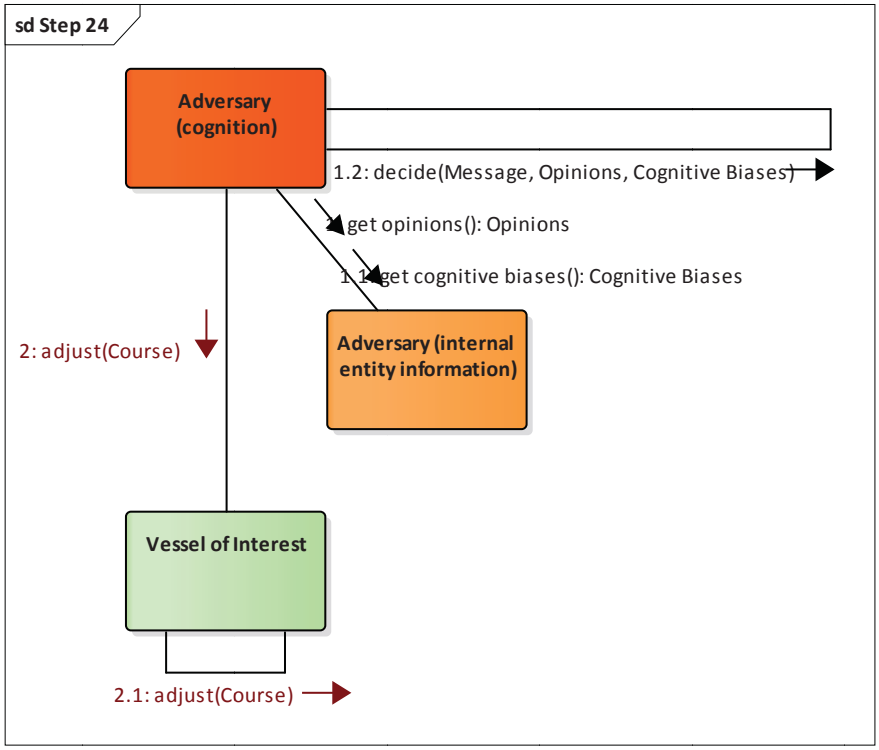

Figure 5-25: Communication Diagram for Step 24

Adversary changes course based on the discussion

5.1.1.25 Step 25

Consider step 25 in the Present OCO Simulation use case: EW Resources track Adversary using EW interception and direction finding (ELINT) of marine radio discussion. Table 5-25 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, all layers in the IWSA are involved.

Table 5-25: Operational Systems and Activities in Step 25

EW Resources track Adversary using EW interception and direction finding (ELINT) of marine radio discussion

Operation System and Activity	Type	Layer
Adversary talks	Action (speak)	Cognition
(remembering the message)	Information	Content
on *Marine Radio equipment* to transmit	Communication System	Conduit
on the *Marine Radio frequencies,*	Communication System	Conduit
whose reception is impacted by the *VOI* and *EW Resources ship* locations	Location	Physical
and is detected by *ELINT sensor*	Detection	Conduit
producing a track	Track	Content
that is viewed by the *EW Resources*	Action (look)	Cognition

Figure 5-26 contains a representation of step 25 as a UML communication diagram.

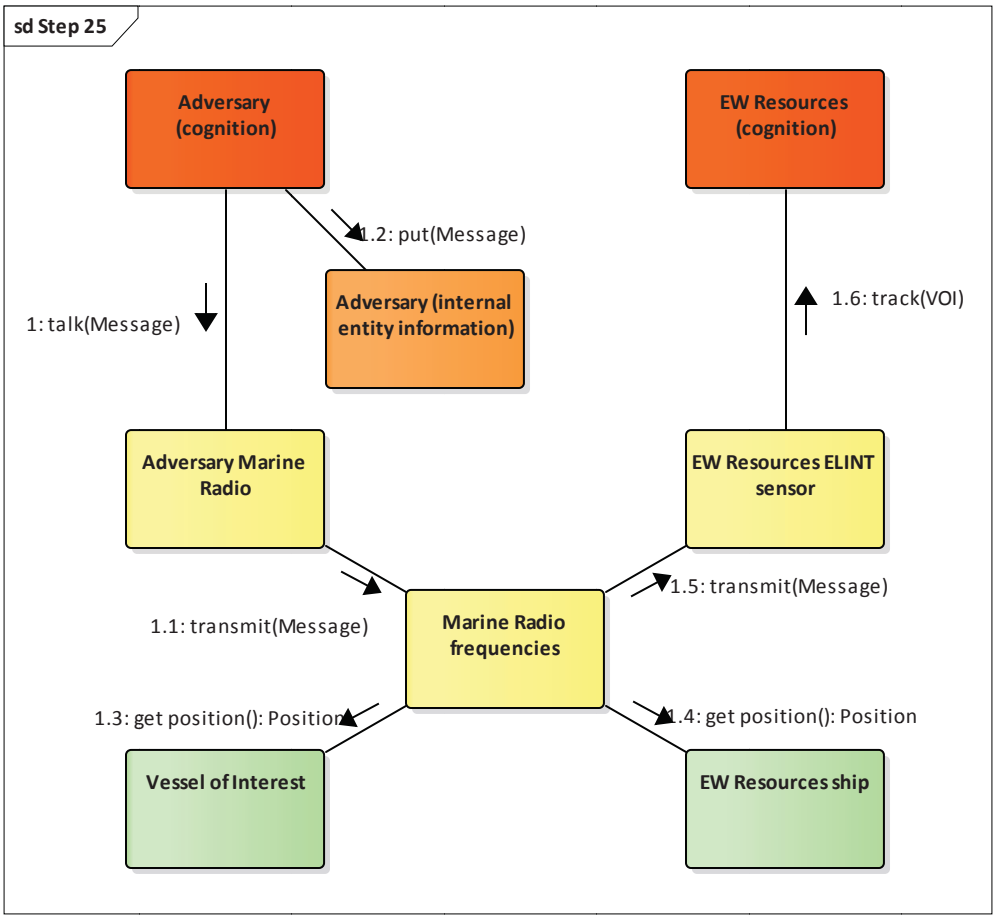

Figure 5-26: Communication Diagram for Step 25

EW Resources track Adversary using EW interception and direction finding (ELINT) of marine radio discussion

5.1.1.26 Step 26

Consider step 26 in the Present OCO Simulation use case: EW Resources jam marine radio of Adversary. Table 5-27 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, the Cognition, Conduit and Physical layers in the IWSA are involved.

Table 5-26: Operational Systems and Activities in Step 26

EW Resources jam marine radio of Adversary

Operation System and Activity	Type	Layer
EW Resources use the *Jammer*	Operate EW system	Cognition Conduit

Operation System and Activity	Type	Layer
to jam the *Marine Radio frequencies* around the *Adversary* location	EW effect Location	Conduit Physical
Adversary hears only noise on *Marine Radio equipment* on the *Marine Radio frequencies* where the jamming performance is impacted by the *VOI* and *EW Resources ship* locations	Action (listen) Communication System Communication System Location	Cognition Conduit Conduit Physical
Adversary talks (remembering the message) on *Marine Radio equipment* to transmit on the *Marine Radio frequencies* and the communication is jammed where the jamming performance is impacted by the *VOI* and *EW Resources ship* locations	Action (speak) Information Communication System Communication System EW effect Location	Cognition Content Conduit Conduit Conduit Physical

Figure 5-27 contains a representation of step 26 as a UML communication diagram.

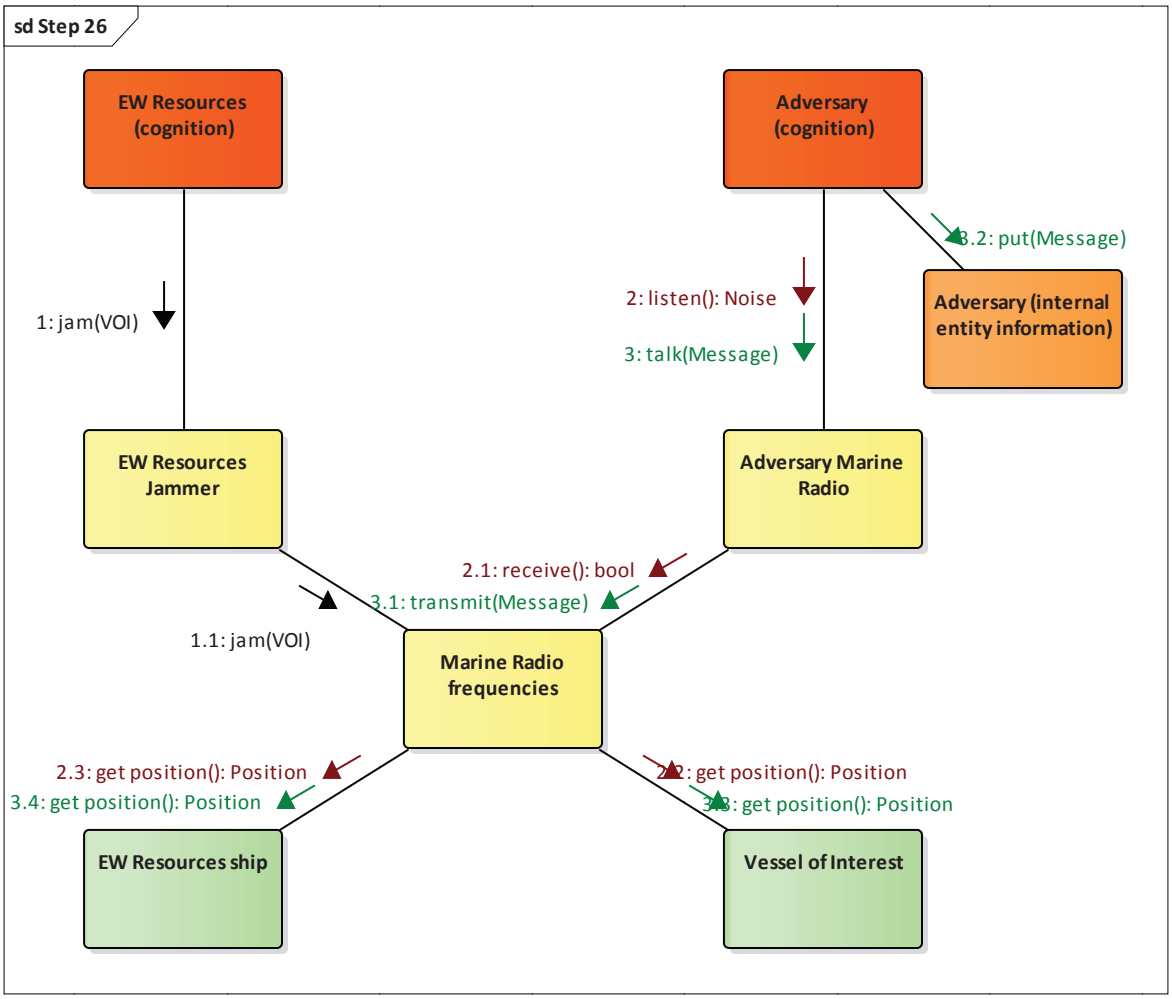

Figure 5-27: Communication Diagram for Step 26

EW Resources jam marine radio of Adversary

5.1.1.27 Step 27

Consider step 27 in the Present OCO Simulation use case: When in detection range, TG detect then track Adversary by radar then EO/IR then visual. Table 5-27 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, the Physical and Cognition layers in the IWSA are involved. The Conduit and Content layers (e.g., the systems forming the COP) have been omitted for clarity.

Table 5-27: Operational Systems and Activities in Step 27

When in detection range, TG detect then track Adversary by radar then EO/IR then visual

Operation System and Activity	Type	Layer
TG ships navigate to intercept Adversary	Movement	Physical
TG ships detect VOI using *Tracking Radar* *CTG Staff* orders course adjustment *TG ships* adjust course	Detection Action (Command) Movement	Physical Cognition Physical
TG ships detect VOI using *EO/IR* *TG ships* maintain course	Detection Movement	Physical Physical
TG ships detect VOI *Visually* *TG ships* maintain course	Detection Movement	Physical Physical

Figure 5-28 contains a representation of step 27 as a UML communication diagram. Note that the result of omitting the Conduit and Content layer activities in this step result in a representation that is a lower fidelity than the communication and cyber elements in the earlier steps.

Figure 5-29 contains an enhanced representation of step 27 as a UML communication diagram that does include Conduit and Content layer activities, which demonstrates the additional complexity of modelling the additional components. Note that Figure 5-29 is still not complete, the *EW Resources ship* components have been omitted to ensure the diagram is legible.

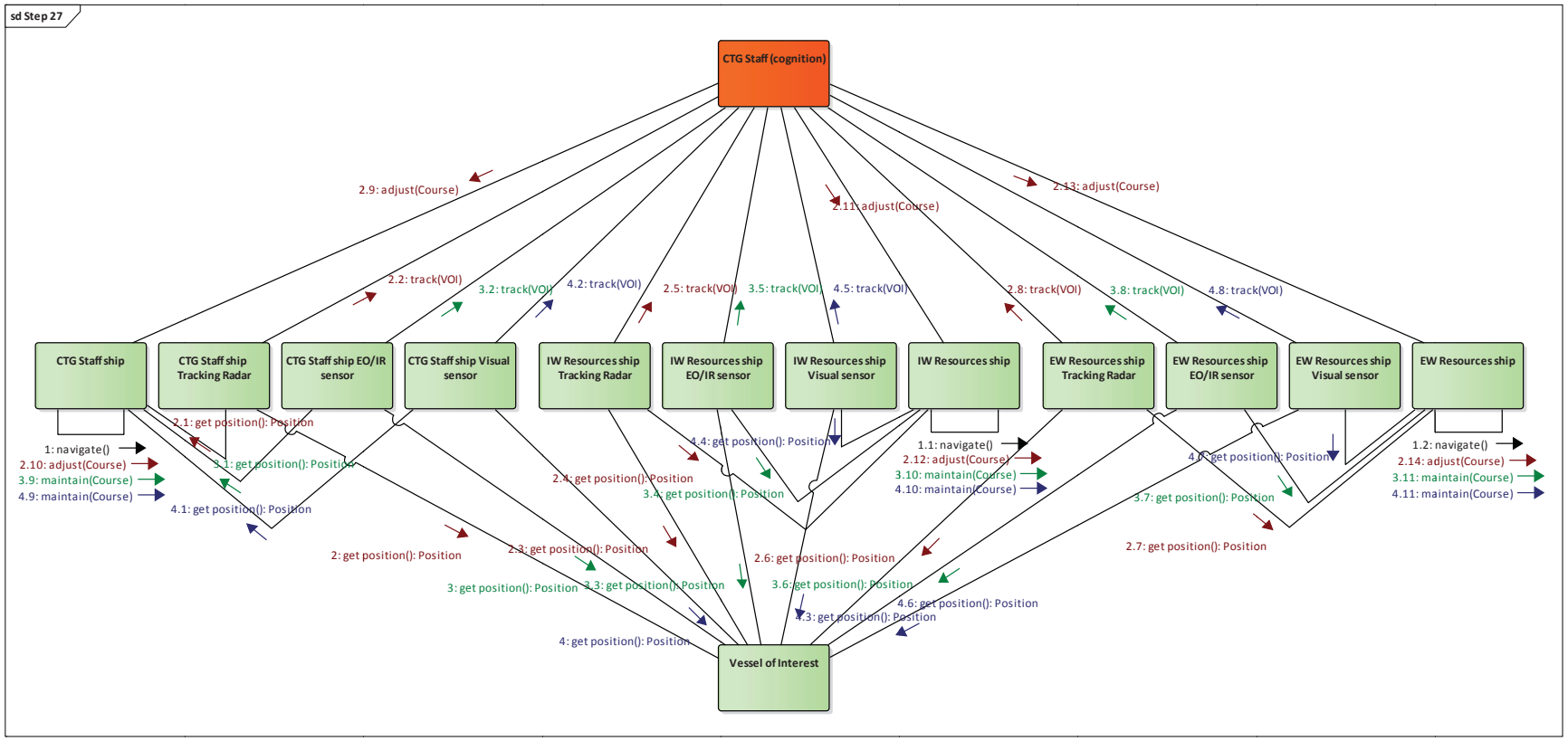

Figure 5-28: Communication Diagram for Step 27

When in detection range, TG detect then track Adversary by radar then EO/IR then visual; the Conduit and Content layer elements have been omitted for clarity

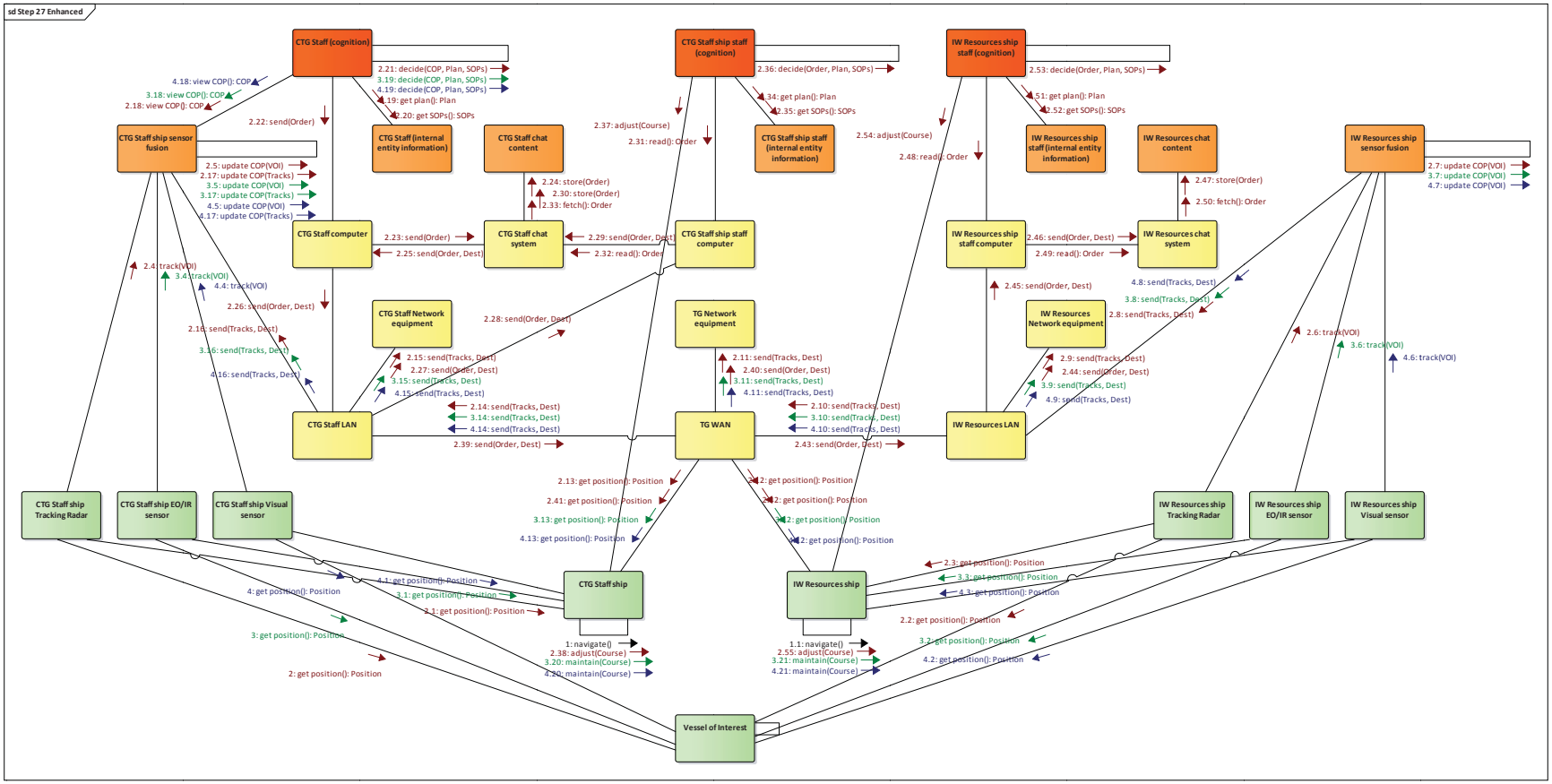

Figure 5-29: Enhanced Communication Diagram for Step 27 (with EW Resources Ship Components Omitted)

When in detection range, TG detect then track Adversary by radar then EO/IR then visual; the Conduit and Content layer elements have been omitted for clarity

5.1.1.28 Step 28

Consider step 28 in the Present OCO Simulation use case: TG intercepts Adversary and the training scenario concludes. Table 5-28 decomposes this into the operational systems, activities and information, the type of the operational system or activity, and the layer in the IWSA involved at each stage. In this step, the Physical and Cognition layers in the IWSA are involved.

Table 5-28: Operational Systems and Activities in Step 28

TG intercepts Adversary and the training scenario concludes

Operation System and Activity	Type	Layer
CTG Staff orders boarding party to board the VOI and detain the Adversary	Action (Command)	Cognition
Boarding party boards the VOI	Movement	Physical
Boarding party detains the Adversary	Movement	Physical

Figure 5-30 contains a representation of step 28 as a UML communication diagram.

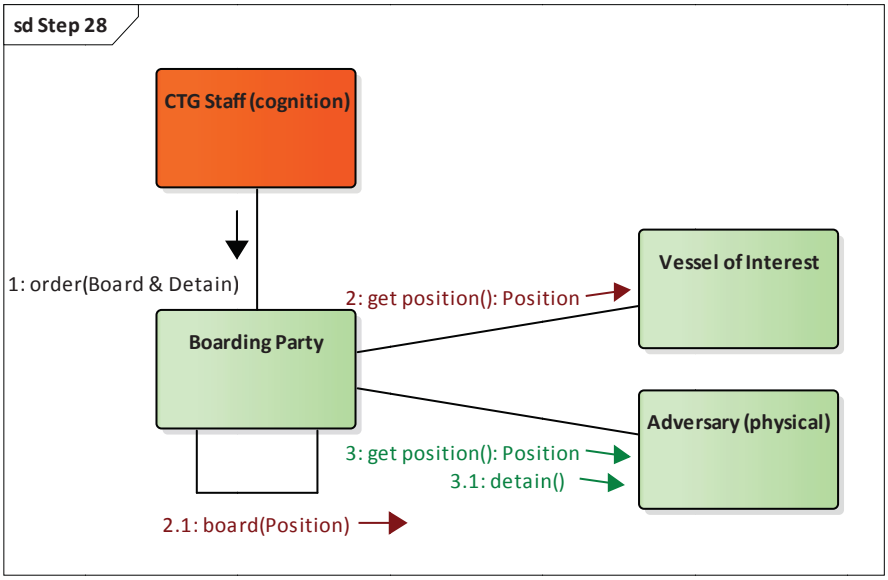

Figure 5-30: Communication Diagram for Step 28

TG intercepts Adversary and the training scenario concludes

5.1.1.29 Step 29

Step 29 in the Present OCO Simulation use case is not included as a part of this analysis, as it consists of after-action review and evaluation rather than activities that are simulated.

5.1.2 Observations

Based on our decomposition of the steps in the Present OCO Simulation use case, we make the following observations.

5.1.2.1 OODA Loop

We have characterised the activities of the Cognition layer using the four elements of Boyd's OODA Loop (Observe, Orient, Decide, Act) (Boyd, 1995) (Osinga, 2005). The Observe, Orient and Decide elements all receive or process information held in the Content layer, either as Entity Internal Information (memory) or externally within an Information System. However, the Act element, represented by the issuing of commands and other actions, can affect more than just the Content layer, in the case where the action directly affects something in the Conduit or Physical layers. As such, the Cognition layer clearly sits at the "top" of the IWSA hierarchy.

5.1.2.2 Patterns

There is a definite pattern in the relationship between a decision maker (or particular computer applications such as the Malware), the manipulation, use and propagation of information content (including e-mail and social media content), and methods of communication (including fixed LANs, Wi-Fi networks, the internet and cell phone networks). The interfaces between these components are conceptually the same or very similar.

Figure 5-31 contains a pattern for a decision maker operating a device running communications software to create some content and then send it towards a recipient. Using the Present OCO Simulation use case as an example, the device can be a computer or cell phone; the communications software can be for e-mail, chat, SMS, Facebook messages, Twitter messages, Instagram messages or Signal messages; the network can be a wired or wireless LAN, a WAN, the Internet or a cell phone network. The same pattern can also be adapted for voice (calls) if message creation and sending is combined and the content is not (necessarily) stored.

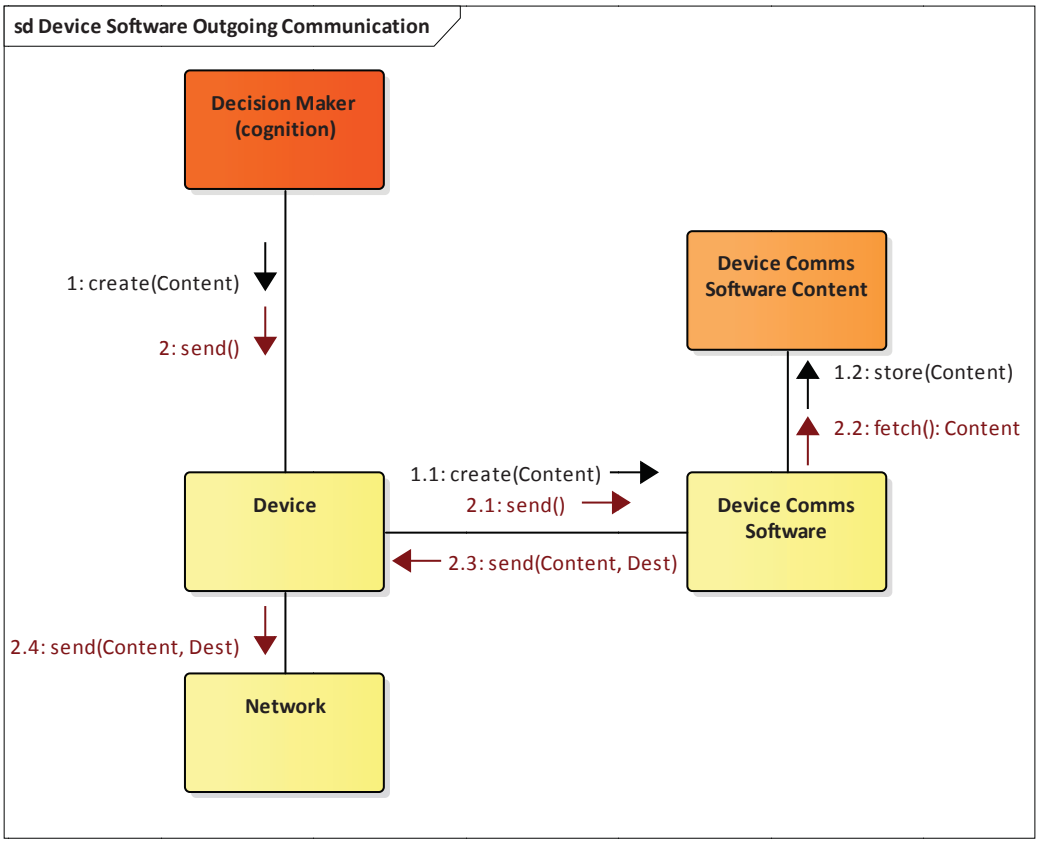

Figure 5-31: Communication Diagram for the Device Software Outgoing Communication Pattern

Figure 5-32 contains a pattern for a sending data over a network. The pattern takes network properties and physical elements into account, as needed. Using the Present OCO Simulation use case as an example, the network can be a fixed LAN, wireless LAN, WAN, the Internet or a cell phone network; the source and destination can be computers, cell phones, or other networks; the network equipment can be specific networking hardware or an organisation providing such as service such as an ISP; the physical element of the source and destination can be a position in the case of a wireless network or the status (or presence) of specific hardware for wired networks.

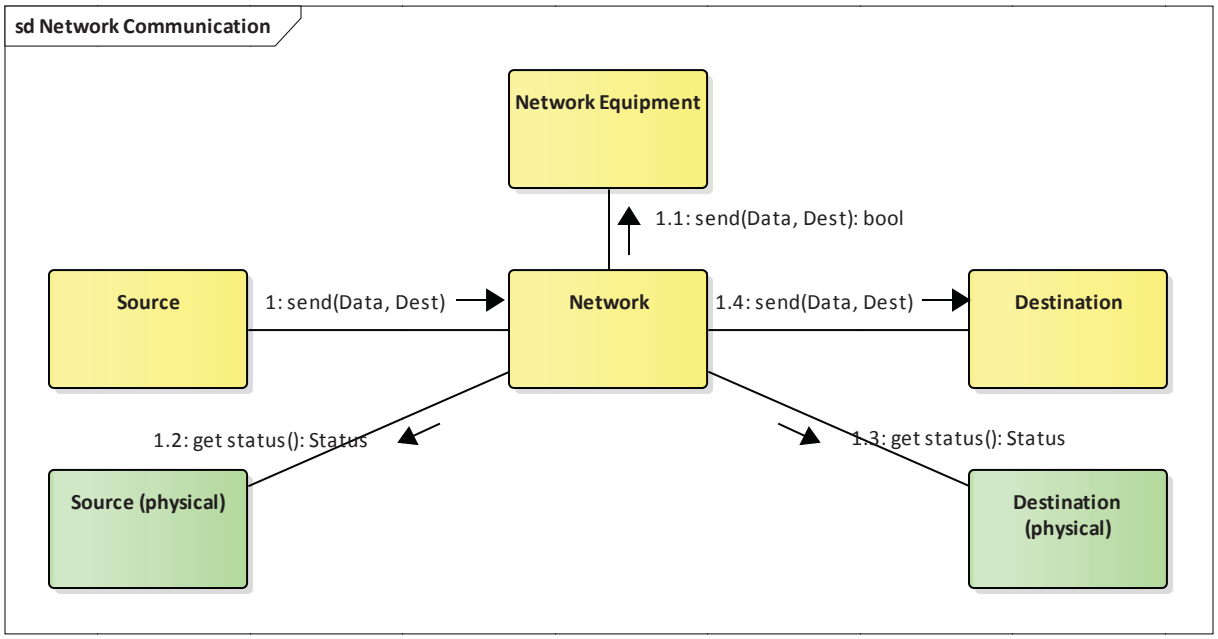

Figure 5-32: Communication Diagram for the Network Communication Pattern

Figure 5-33 contains a pattern for a decision maker operating a device running communications software to receive content. Using the Present OCO Simulation use case as an example, the device can be a computer or cell phone; the communications software can be for e-mail, chat, SMS, Facebook messages, Twitter messages, Instagram messages or Signal messages; the network can be a wired or wireless LAN, a WAN, the Internet or a cell phone network. The same pattern can also be adapted for voice (calls) if message sending and reading is combined and the content is not (necessarily) stored.

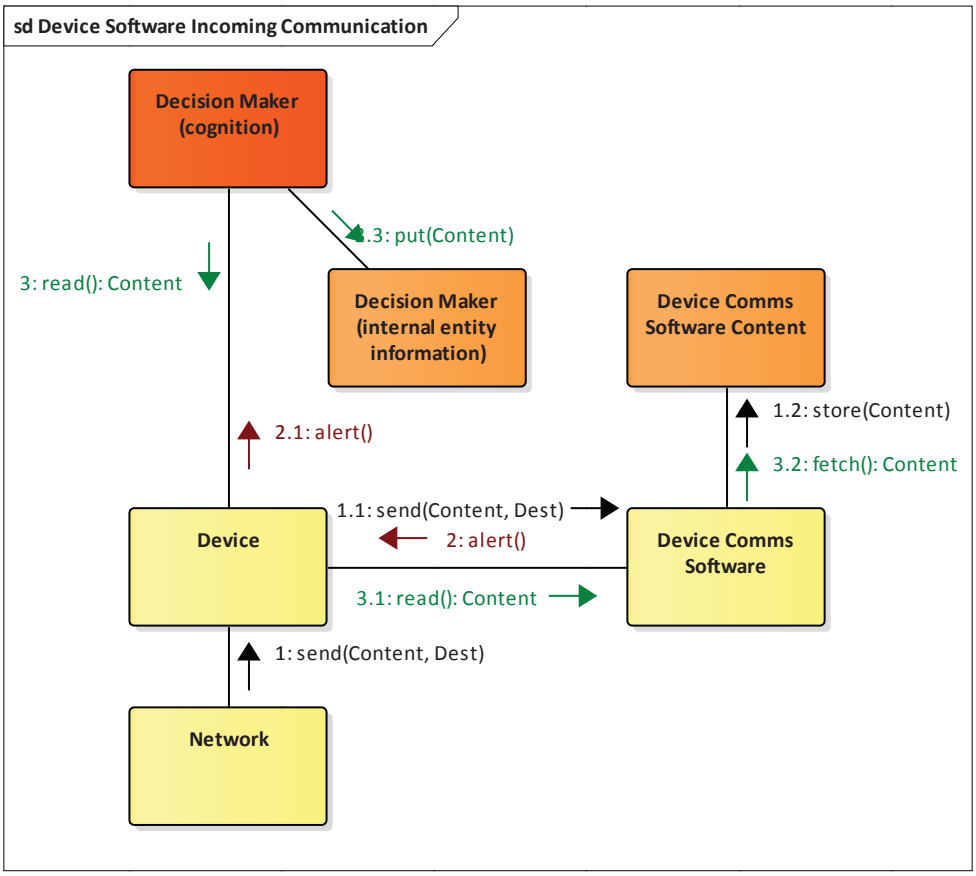

Figure 5-33: Communication Diagram for the Device Software Incoming Communication Pattern

When combined, these three patterns can create a complete end-to-end communication pattern for the transmission of content (messages of different types and voice) between two decision makers.

Variations on these patterns can have software (such as the malware) replace the decision maker in sending messages, and other computer or information systems (such as websites) replace the decision maker in receiving messages.

Patterns such as those presented in Figure 5-31, Figure 5-32 and Figure 5-33 are extremely useful in accelerating the analysis of use cases and ensuring that they are presented in a consistent manner. We recommend that these patterns be used in the analysis of future use cases in other domains.

5.1.2.3 Content and Conduit Layer Relationship

The relationship between the Content and Conduit layers can be seen as more complex than a simple hierarchy. We consider that the Content layer contains information systems (which can be computer systems) and the Conduit layer contains the means to move data from one

physical or logical location to another (which can also include computer systems). Elements of the Conduit layer clearly have a location and representation in the Physical layer (as equipment). However, nodes in the Conduit layer can also be computer systems of varying complexity (e.g., including switches and routers up to full computer systems) and subject to the same vulnerabilities as similar elements in the Content layer. As a result, we believe that the Content layer will use the Conduit layer to transport information, and elements of the Conduit layer can also have a representation in the Content layer for the storage and interpretation of content and configuration data.

5.2 Architecture Layer Internal Interfaces

Within each of the layers of the IWSA, there are a number of different models that may apply, either directly in terms of providing guidance or a definition for developing internal interfaces, or indirectly in terms of a model to think about its contents and behaviour in general terms. In this section, we briefly review models that apply to the Conduit, Content, and Cognition layers.

5.2.1 Conduit Layer

> "The nice thing about standards is that you have so many to choose from"
>
> – Andrew S. Tanenbaum, *Computer Networks,* p168 (Tanenbaum, 1981)

5.2.1.1 Open Systems Interconnection Model

The Open Systems Interconnection (OSI) model for computer networking (ISO/IEC, 1994) is a seven layer model which defines layers ranging from a Physical Layer (Layer 1) to an Application Layer (Layer 7). Table 5-29 shows the layers of the OSI model and provides examples (Wikipedia, 2017) of standards and protocols that are examples of technologies within each of those layers.

Relating the OSI model to the IWSA, the components of the Physical Layer (Layer 1) could be considered to reside within the Physical layer of the IWSA, but communication within the Physical Layer (Layer 1) resides within the Conduit layer of the IWSA.

At the other end, the components of the Application Layer (Layer 7) of the OSI model remain within the Conduit layer of the IWSA, providing services to move information in the Content layer of the IWSA from one physical or logical location to another.

Table 5-29: Layers of the OSI Model

Layer	Name	Examples
Layer 7	Application Layer	DNS, HTTP, SMTP, FTP, NNTP, NFS, DHCP
Layer 6	Presentation Layer	XML serialisation, MIME, SSL, TLS, MPEG
Layer 5	Session Layer	Sockets

Layer	Name	Examples
Layer 4	Transport Layer	TCP, UDP
Layer 3	Network Layer	IP, IPsec, ICMP, IPv4 addresses, IPv6 addresses
Layer 2	Data Link Layer	Ethernet, Ethernet MAC addresses, FDDI, PPP
Layer 1	Physical Layer	1000BASE-TX, IEEE 802.11 PHY, RJ45, RS-232C

5.2.1.2 RFC 1122 TCP/IP

The Request for Comments (RFC) 1122 document entitled *Requirements for Internet Hosts – Communication Layers* (Internet Engineering Task Force, 1989) produced by the Internet Engineering Task Force (IETF) contains a four layer model which defines layers ranging from a Link Layer (Layer 1) to an Application Layer (Layer 4). This model is simpler than the OSI model. Table 5-30 shows the layers described by RFC 1122 and provides examples (Wikipedia, 2017) of standards and protocols that are examples of technologies within each of those layers.

Relating this four layer model to the IWSA, this model is encapsulated entirely by the Conduit layer of the IWSA. The Link Layer (Layer 1), which is the lowest level layer, is purely a communications layer and does not have any physical elements. At the other end, as in the OSI model, the components of the Application Layer (Layer 4) remain within the Conduit layer of the IWSA, providing services to move information in the Content layer of the IWSA from one physical or logical location to another.

Table 5-30: Layers of RFC 1122 (TCP/IP)

Layer	Description	Examples
Layer 4	Application Layer	DHCP, DNS, FTP, HTTP, IMAP, NTP, SMTP
Layer 3	Transport Layer	TCP, UDP
Layer 2	Internet Layer	IP (IPv4, IPv6), ICMP, IPsec
Layer 1	Link Layer	MAC (Ethernet, DSL, ISDN, FDDI), PPP

5.2.2 Content Layer

In contrast to the area of computer network communications, there is no published standard for the layering of computer information. One set of informal models, known as *software stacks* or *solution stacks*, which themselves can be considered to be layers, have been discussed and are in common used (Wikipedia, 2017).

One general software stack consists of: an operating system, middleware, a database, and software applications. A variation on this regards the database as middleware and contains only the other three layers. Within these stacks, there are no single (set of) interface standards between components in use. While some technologies are common (for example, SQL for querying databases), they are by no means universal or consistently applied.

Another popular software stack for web-oriented applications and deployment consists of: an operating system, a web server, a database and a programming language. Table 5-31 contains example instances of this software stack (Wikipedia, 2017). Note that in the context of the IWSA we consider a web service as being a part of the Conduit layer, but its content is a part of the Content layer.

Table 5-31: Web-Oriented Software Stacks

Web-Oriented Software Stack	Examples	
	LAMP	WINS
Programming Language	Perl / Python / PHP	.NET (framework and languages)
Database	MySQL / MariaDB	SQL Server
Web Server	Apache	Internet Information Services
Operating System	Linux	Windows Server

These software stacks are unlikely to be sufficiently rich to appropriately model all applications. For example, consider malware that works by deleting or encrypting files. According to the software stacks above, this would primarily occur in the operating system layer. To model this with sufficient fidelity, it may be appropriate to decompose this into a basic operating system kernel, disk (device) drivers, and a file system with applications (the malware) above this.

In a military context, data formats that represent and contain information may be considered to be a part of the Content layer. For example, the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM), the Variable Message Format (VMF) and Over-The-Horizon (OTH) Targeting Gold (OTG) are relevant data formats. Even information represented using simulation standards such as the Distributed Interactive Simulation (DIS) and High Level Architecture (HLA) can be considered to be part of the Content Layer. However, some of these formats may also be considered to be Conduit formats for the envelope rather than the information content contained within.

5.2.3 Cognition Layer

The Cognition (Decision Making) layer is an example of what has traditionally been regarded as “artificial intelligence”. As a result, cognitive models and proposed implementations from artificial intelligence research could potentially be applied to an implementation of a cognitive simulation model. Historically these have included rule-based systems, expert systems, neural networks, and “intelligent” agents. One may argue that a user interface to a human subject matter exert (SME) also qualifies as an implementation of a decision making model.

The Belief-Desire-Intention (BDI) Model (Bratman, 1987) and the related BDI software architecture (Rao & Georgeff, 1991) provides a foundation for the modelling of decision making using agent technologies. This has been applied to the modelling of human operators in military simulation (Tidhar, et al., 1999).

The OODA Loop (Boyd, 1995) that we used as a framework in section 5.1.1 to characterise the activities of the decision making has been used in conjunction with both the BDI software architecture (Tidhar, et al., 1999), albeit not explicitly (the terms used were Situation Awareness, Situation Assessment, Tactic Selection and Action), and also simpler technologies such as "state machine (SM) agents" in (Selvestrel, Harris, & Ibal, 2004). In our view, it provides an excellent model for thinking about the elements of a decision maker.

In summary, there is no commonly accepted standard for the implementation of decision making models, and it is still an active area of research.

5.3 Inter-Module and Inter-Layer Interfaces

From a pure software architecture standpoint, the inter-module and inter-layer application programming interfaces (APIs) used to implement the IWSA need not be overly complex.

Within existing simulation products and standards, the primary interface patterns between modules (whether they are called modules, models, federates, or some other term) and the simulation infrastructure is a publish/subscribe model for producing and receiving data. They contain separate functions for initialization (or connecting, or creating), termination (or disconnecting, or clean-up), and computation.

For example, in the HLA standard (IEEE, 2010), a federate will connect to and join a federation at the beginning and resign and disconnect at the end through the HLA Run-Time Infrastructure (RTI) (Pitch Technologies, 2014). It will subscribe to data it wants to receive, and publish data that it produces. The data itself is defined in a Federation Object Model (FOM) (IEEE, 2010).

Note that the internals of existing CGF products may be structured differently, and not in a manner consistent with the HLA standard, or any other standard. From a pragmatic standpoint, unless one is developing a new CGF, it is unrealistic to expect that the internal interfaces of a CGF will be changed to conform to any new standard.

Therefore, the most important interface consideration is not the API in use but the data that is transferred between modules and layers. This is the topic of the next section.

6 DATA MODEL

There are a range of different factors that should be taken into account when developing a data model for a simulation architecture. In this section, we leverage the Present OCO Simulation use case to motivate and consider a data model for the interactions and objects used during simulation execution, and to represent the order of battle (ORBAT) used to define and initialize a simulation, all within the context of the layers of the IWSA.

The data model we developed contains interactions, which capture behaviour connecting simulation components and are presented in Section 6.1, and other objects which capture the data sent between simulation objects and are presented in Section 6.3. The simulation components themselves can be used to represent the ORBAT, and this is discussed in Section 6.2.

6.1 Use Case Component Interactions

At an abstract level, the interactions between components in the Present OCO Simulation use case are shown in Figure 5-1 to Figure 5-30. Here we characterise the connections between the components in terms of the interactions between them and the data used by the interactions.

6.1.1 Cognition Layer

Within the use case, components in the Cognition layer interact directly with components in each of the other three layers.

At a basic level, 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 (command operations). The destination component of *commands* and *operate* interactions may be in any of the other three layers, while interactions with *entity internal information* is always an interaction with the Content layer.

Operate interactions may take several forms, arguably the most common of which is based on a physical interaction such as pressing, pushing, pulling, turning and swiping, although the exact form of physical interaction would normally be considered to be too detailed to simulate directly in a CGF. The next most common *operate* interaction is based on a verbal interaction. Other *operate* interactions can be considered to include other forms of movement and eye tracking as a form of signalling.

In the Present OCO Simulation use case, the only explicit *operate* interaction is the (verbal) call made on a cell phone, although the use of computers and cell phones to control software are both implicit *operate* interactions that could be explicitly modelled, if desired.

Interactions with *entity internal information* can broadly be equated to saving and recalling information. It typically corresponds to the Orient and Decide phases of the OODA loop.

The *command* interactions are the most common type of interactions in the use case and encompass issuing commands to both software and other entities. Almost every interaction with software can be seen as a *command* interaction. For example, the creation of e-mail to be sent, sending it, checking for a response and then reading a response can all be seen as *command* interactions. Issuing a *command* to software or a software system may abstract out the device being used (*operate* interactions) or may be modelled as a command to the device which is then passed on to the resulting system.

The *command* and *operate* interactions typically correspond to the Act phase of the OODA loop, although they can also correspond to the Observe phase when related to actively gathering information.

Alternatively, interactions originating within the Cognition layer could be categorised using higher level concepts. For example, many of the interactions in the Present OCO Simulation use case originating within the Cognition layer concern *initiating* or *responding* to messages of various types. These could then be decomposed into interactions that *operate* or are *commands*. It is not clear which representation is best, and it may be application and context dependent. Examining this question in more detail, and other issues within the Cognition layer more generally, is an area for future research.

Table 6-1 summarises the interactions that originate in the Cognition layer using both higher level (*initiate* / *respond*) and lower level (*operate*, *command*) representations.

Table 6-1: Interactions Originating in the Cognition Layer

Cognition Interaction Category	Action Type	Example Actions
Operate	Physical	Move, watch, type
	Verbal	Say, call
Entity Internal Information	Input from	Get, recall, fetch
	Output to	Put, remember, store
Command	Input	Get, fetch, read
	Output	Put, store, write
	Act	Do
Initiate / Respond	Output	Compose, send (say, write)

Note that cognitive elements such as opinions, biases, requests, reports and command hierarchies are parameters to these interactions and are discussed in Section 6.1.5. The “do” command covers an instruction to act in accordance with a Standard Operating Procedure (SOP) and the Rules of Engagement (ROE). In an early draft of this report, some of the physical interactions contained in Table 6-1 were very low level, much lower than typically simulated by existing CGFs and probably too low level to be useful. This reinforces the need for additional research and prototyping for a variety of use cases to get the level of detail as correct as possible.

Interactions that originate in the Content, Conduit and Physical layers that terminate in the Cognition layer can be considered to be interactions whose purpose is to asynchronously alert the Cognition layer of an event or passively provide some form of information. That is, they provide a *signal* to the Cognition layer that something has happened or some data is available. Table 6-2 summarises the interactions that originate in other layers that terminate in the Cognition layer.

Table 6-2: Interactions Originating in Other Layers Terminating in the Cognition Layer

Cognition Interaction Category	Action Type	Example Actions
Signal	Signal	Alarm, notify

6.1.2 Content Layer

Within the use case, components in the Content layer interact directly with components in the Cognition and Conduit layers but not the Physical layer. Computers, software applications, software application content, website content and entity internal information are all examples of components to which these interactions apply.

The interactions originating in the Content layer are essentially the same as the *command* interactions that originate in the Cognition layer. They involve taking input data, producing output data, performing some computation, or a combination of all three. These interactions apply to those that remain within the Content layer and those that originate in the Content layer and terminate in a different layer.

It follows that a general computational signature for these interactions can be considered to be:

Act (Input Data) : Output Data

Examples of this general computational signature commonly used in the Content layer are:

read (What) : Data

store (Data, Where)

send (Data, Where) : bool

Note that these signatures also encapsulate error conditions and a failure to provide or retrieve information in addition to the successful or expected case. That is, the data returned may include error codes, error descriptions or no data (which may indicate no response to a request).

Table 6-3 summarizes the interactions that originate in the Content layer.

Table 6-3: Interactions Originating in the Content Layer

Cognition Interaction Category	Action Type	Example Actions
Command	Input	Fetch, read
	Output	Store, send, upload
	Act	Install, disable, update

Note that the *signal* interactions terminating in the Cognition layer that originate in the Content layer are an example of an *output* message from the perspective of the Content layer.

6.1.3 Conduit Layer

Within the use case, components in the Conduit layer interact directly with components in all four layers.

The purpose of the components within the Conduit layer is to transfer data from one location to another. As such, it follows that the primary interactions occurring within this layer can be characterised as:

send (Data, Destination) : Result

Note that the result that is returned can encapsulate both success status and error conditions.

Other interactions can be built upon this foundation. For example,

get (What, Where From) : Data

can be considered to be

[Requester] send ((Get, What, Requester), Where From)

[Where From] send (Data, Requester)

Nevertheless, it is helpful to be able to consider higher level interactions than simply decomposing all interactions into a sequence of *send* operations.

The other interactions originating in the Conduit layer that are directed at both the Conduit layer and other layers are similar to those that originate in the Content layer, as discussed in Section 6.1.2. Table 6-4 summarizes the interactions that can originate in the Conduit layer. The interactions listed in *italics* are additional interactions not explicitly specified in the Present OCO Simulation use case.

Table 6-4: Interactions Originating in the Conduit Layer

Cognition Interaction Category	Action Type	Example Actions

Cognition Interaction Category	Action Type	Example Actions
Command	Input	Get, fetch, download
	Output	Send, store, post, tweet, call, transmit
	Act	Create, open, connect, install, jam, *close, control*
Status	Output	Error

Note that, as in the Content layer, the *signal* interactions terminating in the Cognition layer that originate in the Conduit layer are an example of an *output* message from the perspective of the Conduit layer.

6.1.4 Physical Layer

Within the use case, components in the Physical layer interact directly with components in the Cognition and Conduit layers. A primary interaction is to provide the geolocated positional information of an entity or component as a service in response to a *query*.

A number of the interactions originating within the Physical layer in the Present OCO Simulation use case are the same or similar to interactions originating in higher layers, such as the Cognition layer. A *query* for the position of an entity can originate in the Physical layer, and also conceptually in each of the other layers.

Command interactions that originate in the Physical layer can cover simple movement instructions for different types of entities, including personnel, land vehicles, maritime vessels and aircraft. They are often lower level (simpler and more specific) than similar commands that originate in the Cognition layer. They can also cover more complex manoeuvres that are encapsulated by SOPs.

Sensor interactions originating in the Physical layer cover detections and tracks that are output to other layers.

Table 6-5 summarises interactions that can originate in the Physical layer. The interactions listed in *italics* are additional interactions not explicitly specified in the Present OCO Simulation use case but are conceptually the same as those present in the Conduit layer.

Table 6-5: Interactions Originating in the Physical Layer

Cognition Interaction Category	Action Type	Example Actions
Location	Query	Get position
Command	Vessel Movement	Navigate, adjust course, maintain course
	Personnel Activity	Board, detain
Sensor	Output	Track

Cognition Interaction Category	Action Type	Example Actions
Status	Output	*Status, error*
	Query	*Get status*

Note that the *track* interactions terminating in the Cognition layer that originate in the Physical layer are an example of a *signal* message from the perspective of the Cognition layer. In the context of the Physical layer, status and error messages allow information such as morale, battle damage assessment to be output to components in other layers.

Table 6-6 summarizes the interactions that can originate in other layers targeted at the Physical layer. Note that there are no sensor commands explicitly referenced in the Present OCO Simulation use case.

Table 6-6: Interactions Originating in Other Layers Targeted at the Physical Layer

Cognition Interaction Category	Action Type	Example Actions
Location	Query	Get position
Command	Vessel Movement	Move, sail, adjust course
	Personnel Activity	Board & detain
	Sensor	*Set mode*

6.1.5 Object Data

In addition to interactions, the other type of data in a simulation data model are the objects that the interactions depend or operate upon. This may be ephemeral, such as a location in the world, represented physically such as an order or report that may be printed on paper, or purely electronic, such as computer data or computer software.

Table 6-7 contains the object data referred to explicitly in the Present OCO Simulation use case categorised by the layer in which the object data (primarily) belongs. It also contains additional related object data listed in *italics* that was not explicitly referred to in the use case.

Table 6-7: Object Data Used in the Present OCO Simulation Use Case

Layer	Subcategory	Object Data
Cognition		Request Response Voice message (live) *Morale*
Content	Military C2	Order Task

Layer	Subcategory	Object Data
		Plan Report SOPs ROE Organizational structure (command hierarchy) COP *Battle damage assessment*
	Electronic message	E-mail message Chat message
	Cell phone	SMS message Voice recording
	COMINT	Recording (message)
	World Wide Web	Web page
		Uniform Resource Locator (URL)
		Software (malware)
	Social media	Facebook message
		Tweet (twitter message)
		Instagram post
	Entity Internal Information	Opinion Cognitive biases
Conduit	Status	Connection (link) status *Communications node status* *Malware communication status* *Error status* *Jamming status*
	ELINT	Track (sensor report)
Physical	Position	Location
	Sensor	Track (sensor report)

6.1.6 Truth and Perceived Data

Within the description of the Present OCO Simulation use case, there is no explicit distinction made between truth data, perceived data, and simulation management data.

We consider *truth data* to be data that is a part of the simulation that reflects the “real world” of the simulation. For example, the actual position of an entity, the state of the environment, and

the actual data stored within an information system all constitute “true” values for those simulated components.

We consider *perceived data* to be data that is part of the simulation that is sensed, interpreted by, or is from the perspective of another entity or component within the simulation. For example, the position of an entity as perceived by a person (using a visual sensor) or equipment (radar), the state of the environment as measured by a simulated weather station, or a person’s interpretation or memory of data stored within an information system all constitute “perceived” values for those simulated components. For any given piece of data, there is only one “true” value but there may be many different “perceived” values, potentially a different perceived value for each entity or component perceiving the data.

While truth data obviously becomes perceived data when interpreted by another entity or component, perceived data can also become (a different) form of truth data. For example, a sensor such as a radar detects an entity, it generates perceived data (a track) that represents the actual (truth data) position of the entity. However, when stored in a C2 system, the track becomes actual (truth) data from the perspective of the simulation of the C2 system. Another simulated entity may then have a (perceived) view of the (true) track, which is also a (perceived) view of the (true) position of the detected entity.

We consider *simulation management data* to be data used to manage the simulation that is not a part of the simulated world. It is a separate collection of data that is maintained and used independently of the truth and perceived data that is modelled within a simulation.

Time is an example of data used within a simulation that could be represented as truth data, perceived data, and simulation management data. For example, the actual time being simulated is truth data, the time as perceived by a simulated entity is perceived data, while the time the simulation has been running and its frequency of update is simulation management data.

We believe that it is very important to distinguish between each of the three types of data. The data model for simulation management data should be considered to be distinct from truth and perceived data. In contrast, as both truth and perceived data are part of the simulation, they should be considered together in a single data model.

Similarly, we believe that, for perceived data, it is equally important that who or what is perceiving the data is known and (potentially) represented.

Many CGFs do not make this distinction between truth and perceived data today. We believe that supporting this should be a part of a CGF architecture and considered at design time, as it is typically difficult and time consuming to add to a completed simulation.

6.2 Use Case Order of Battle

We have decomposed an example conceptual ORBAT structure for the Present OCO Simulation use case into multiple figures. Figure 6-1 shows the ORBAT structure containing the CTG ship. Figure 6-2 shows the ORBAT structure containing the IW Resources ship. Figure 6-3 shows the ORBAT structure containing the EW Resources ship. Figure 6-4 shows the ORBAT

structure containing the other Task Group and Joint HQ (Friendly) elements. Figure 6-5 shows the ORBAT structure containing the Hostage smugglers (Hostile) elements. Figure 6-6 shows the ORBAT structure containing the Neutral elements.

In each of these figures, elements that are simulated by Live components are shown in **bold blue**, while elements that are simulated by Live or Virtual components are shown in *green italics*. All other elements are simulated by Constructive components. Elements that are considered to be data, attributes or parameters of other elements are shown in [brackets].

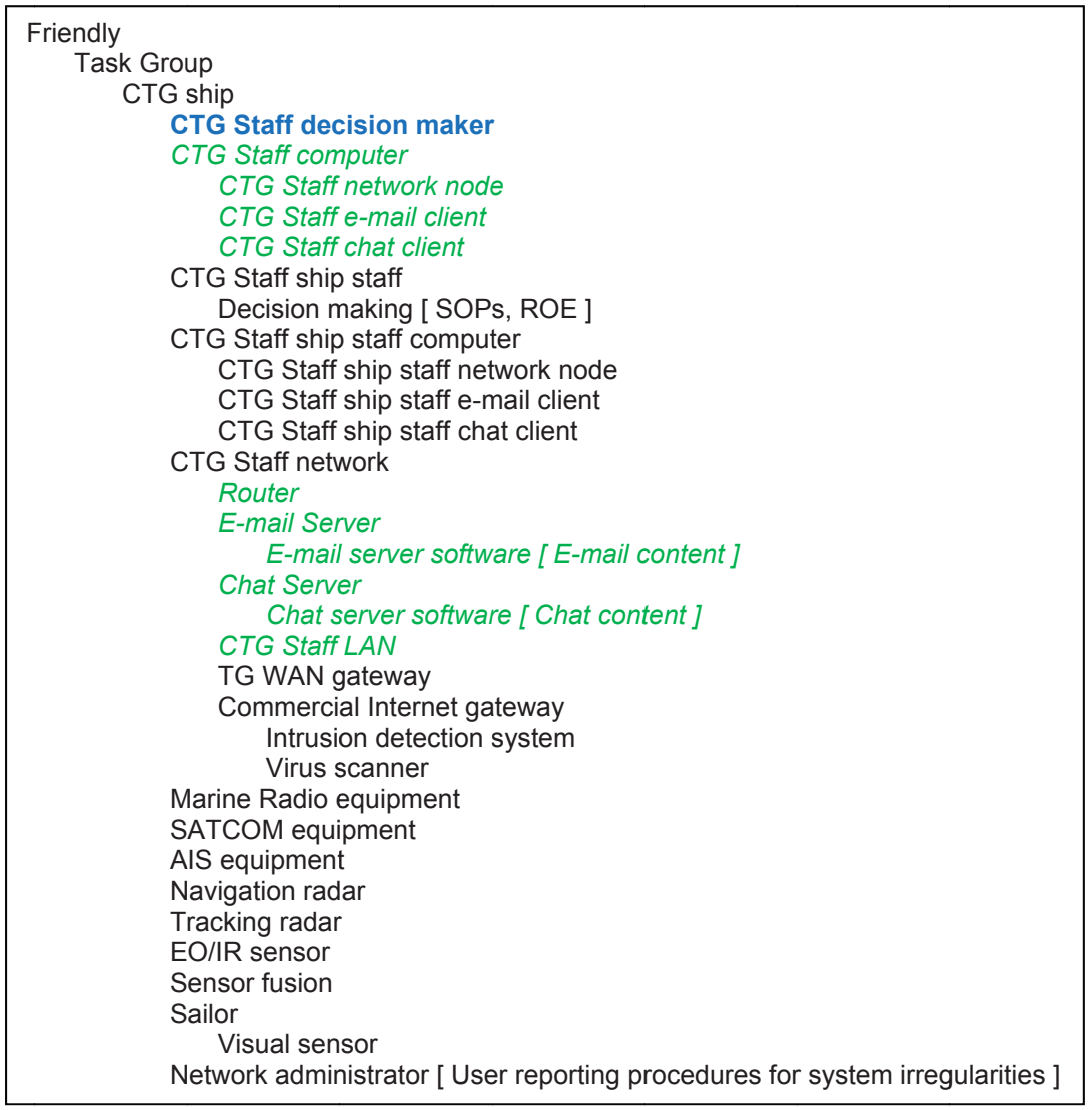

Figure 6-1: Present OCO Simulation Use Case ORBAT: CTG Ship

Friendly (cont.)
- Task Group (cont.)
  - IW Resources ship
    - IW Resources decision maker
      - Decision making [Social media tracking, SOPs, ROE, Opinions, Cognitive biases]
    - IW Resources computer
      - IW Resources network node
      - IW Resources e-mail client
      - IW Resources chat client
      - IW Resources web browser
    - IW Resources cell phone
      - IW Resources Facebook app [Facebook content]
      - IW Resources Twitter app [Twitter content]
      - IW Resources Instagram app [Instagram content]
    - IW Resources ship staff
      - Decision making [SOPs, ROE]
    - IW Resources ship staff computer
      - IW Resources ship staff network node
      - IW Resources ship staff e-mail client
      - IW Resources ship staff chat client
    - IW Resources network
      - Router
      - E-mail Server
        - E-mail server software [E-mail content]
      - Chat Server
        - Chat server software [Chat content]
      - IW Resources LAN
      - TG WAN gateway
      - Commercial Internet gateway
        - Intrusion detection system
        - Virus scanner
    - Marine Radio equipment
    - SATCOM equipment
    - AIS equipment
    - Navigation radar
    - Tracking radar
    - EO/IR sensor
    - Sensor fusion
    - Sailor
      - Visual sensor
    - Sailor
      - HUMINT procedures
    - Network administrator
      - Decision making [User reporting procedures for system irregularities]

Figure 6-2: Present OCO Simulation Use Case ORBAT: IW Resources Ship

Friendly (cont.)
- Task Group (cont.)
  - EW Resources ship
    - EW Resources decision maker
      - Decision making [EW SOPs, ROE]
    - EW Resources computer
      - EW Resources network node
      - EW Resources e-mail client
      - EW Resources chat client
    - EW Resources ship staff
      - Decision making [SOPs, ROE]
    - EW Resources ship staff computer
      - EW Resources ship staff network node
      - EW Resources ship staff e-mail client
      - EW Resources ship staff chat client
    - EW Resources network
      - Router
      - E-mail Server
        - E-mail server software [E-mail content]
      - Chat Server
        - Chat server software [Chat content]
      - IW Resources LAN
      - TG WAN gateway
      - Commercial Internet gateway
        - Intrusion detection system
        - Virus scanner
    - Marine Radio equipment
    - SATCOM equipment
    - AIS equipment
    - Navigation radar
    - Tracking radar
    - EO/IR sensor
    - COMINT sensor
    - ELINT sensor
    - SIGINT sensor
    - Jammer
    - Sailor
      - Visual sensor
    - Network administrator
      - Decision making [User reporting procedures for system irregularities]

Figure 6-3: Present OCO Simulation Use Case ORBAT: EW Resources Ship

- Friendly (cont.)
  - Task Group (cont.)
    - Joint HQ
      - Joint HQ decision maker
        - Decision making [Organizational Structure, SOPs, ROE]
      - Joint HQ computer
        - Joint HQ network node
        - Joint HQ e-mail client
      - Joint HQ network
        - Router
        - E-mail Server
          - E-mail server software [E-mail content]
        - Joint HQ LAN
        - TG WAN gateway
        - Commercial Internet gateway
          - Intrusion detection system
          - Virus scanner
    - TG WAN
    - Internet
      - Website #1
        - Internet node
        - Web service [Website content]
        - Malware
      - Website #2
        - Internet node
        - Web service [Website content]
    - SATCOM network
    - AIS network

Figure 6-4: Present OCO Simulation Use Case ORBAT: Other Task Group Elements

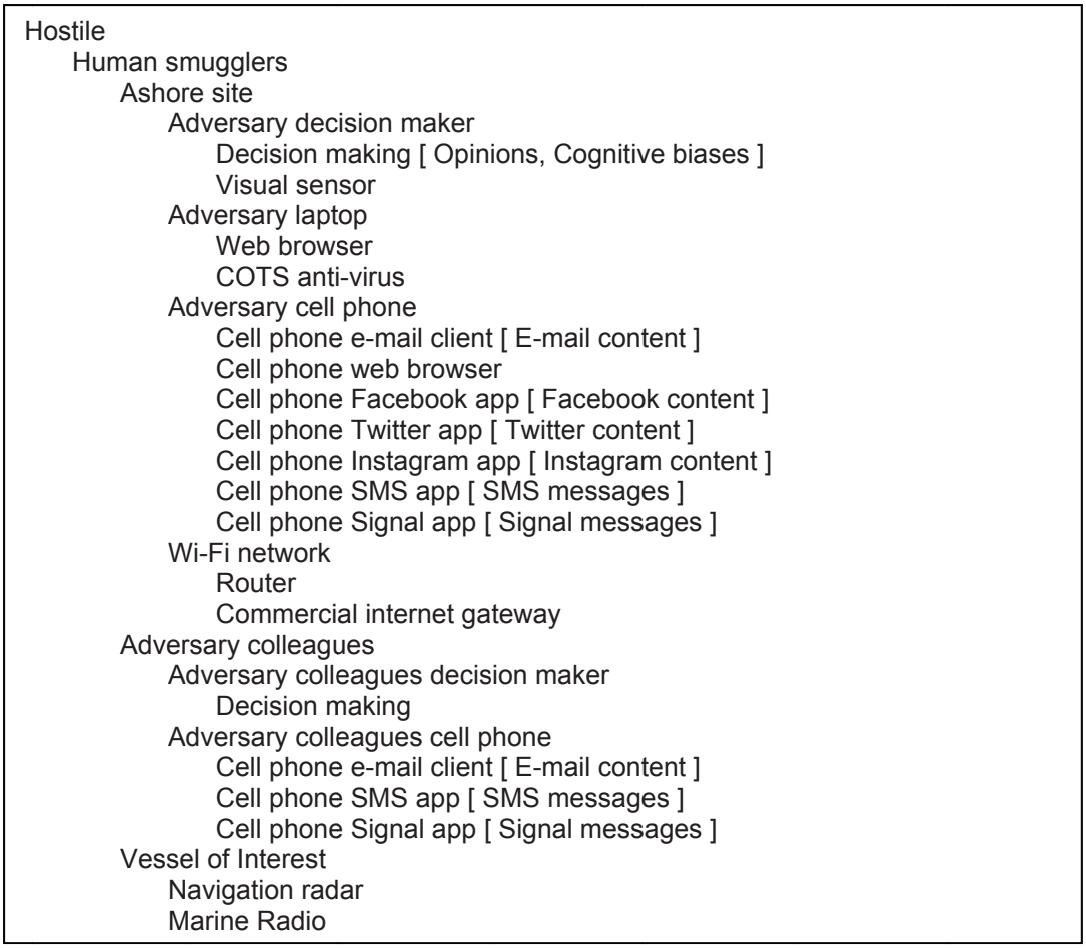

Figure 6-5: Present OCO Simulation Use Case ORBAT: Human Smugglers

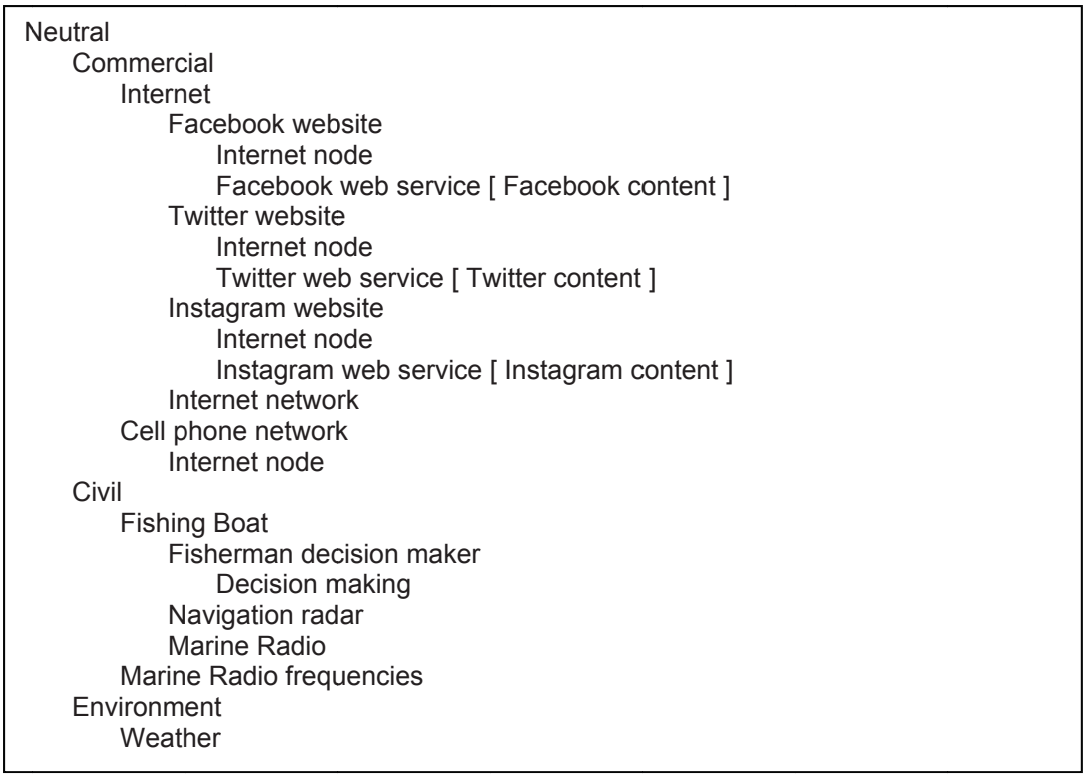

Figure 6-6: Present OCO Simulation Use Case ORBAT: Neutral Elements

6.3 Information Warfare Simulation Data Model

In this section we present a preliminary Information Warfare Simulation Data Model (IWSDM). The primary purpose of the IWSDM presented here is to provide an example representation of elements of the IWSA that are not well represented within existing data models that have been standardized or proposed for standardization and supports the Present OCO Simulation use case.

The IWSDM presented here is intended to support both the definition and initialization of the simulation, as represented by the ORBAT, and the simulation run-time that addresses the interactions occurring throughout the simulation and the data that is passed, especially between the layers. For legibility, we introduce the salient elements in logical groups, rather than attempting to represent the whole model in a single diagram.

Note that many of the names of the elements (classes, enumerations) of the IWSDM contain spaces, and as such do not conform to a representation supported by typical programming languages. Conversion into such a form is an exercise for the reader.

6.3.1 Base Simulation Object

In determining features required of the base *Simulation Object*, which is to be the root object for the IWSDM 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 (ORBAT construction). To facilitate this, we believe that each *Simulation Object* should encapsulate three concepts.

The first concept is that, as discussed in Section 4.2.3, 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 Section 4.2.4.

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 the IWSDM, we represent these three concepts as enumerations and simple attributes of the base *Simulation Object*. It is shown in Figure 6-7. Alternative approaches could use interfaces, methods or abstract methods, or multiple inheritance.

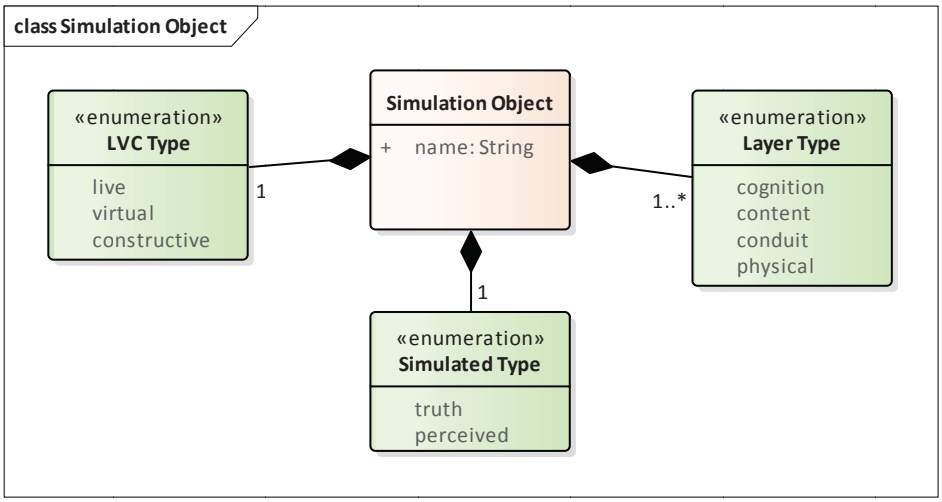

Figure 6-7: Class Diagram for the Simulation Object Class of the IWSDM

We note that the HLA FOM contains only the name in the base object. Further work, including prototyping, should be undertaken on the IWSDM to determine the value of the additional attributes and the degree to which they would be used in practice.

6.3.2 Message Objects

Figure 6-8 shows a class diagram containing *Message* objects in the IWSDM. The *Message* class is a base class for all messages, including formatted messages and web pages, that may be sent between other objects in the simulation. It extends the *Information* class.[5] Each of the different types of verbal, text and multimedia messages sent in the Present OCO Simulation use case are represented. Also shown is a representation of the payload (attachments) of multimedia messages and web pages. We note that video data is not explicitly referenced in the Present OCO Simulation use case but it has been included in Figure 6-8 as another example of multimedia data.[6] Figure 6-8 does not show all of the possible attributes of each class. The *Message* contains two basic attributes (*author* and *message*), but it and all of the other classes may contain additional attributes. For example, for many message types, a *recipient* or *intended recipient* would also be an expected attribute, although it is unlikely that this attribute would be sufficiently universal to apply to the *Message* class.

While objects of the classes shown in Figure 6-8 will be very commonly used at run-time during simulation execution, they may also be used in the ORBAT to define the initial state of the scenario. For example, an e-mail system containing a number of messages at simulation initialization time may have those messages defined as objects of the classes shown in Figure 6-8.

[5] The *Information* class is present to allow for compatibility with other data models. Currently no other classes in the IWSDM extend it.
[6] Whether this is sufficient for all types of video data, including streaming video, is an area for future research.

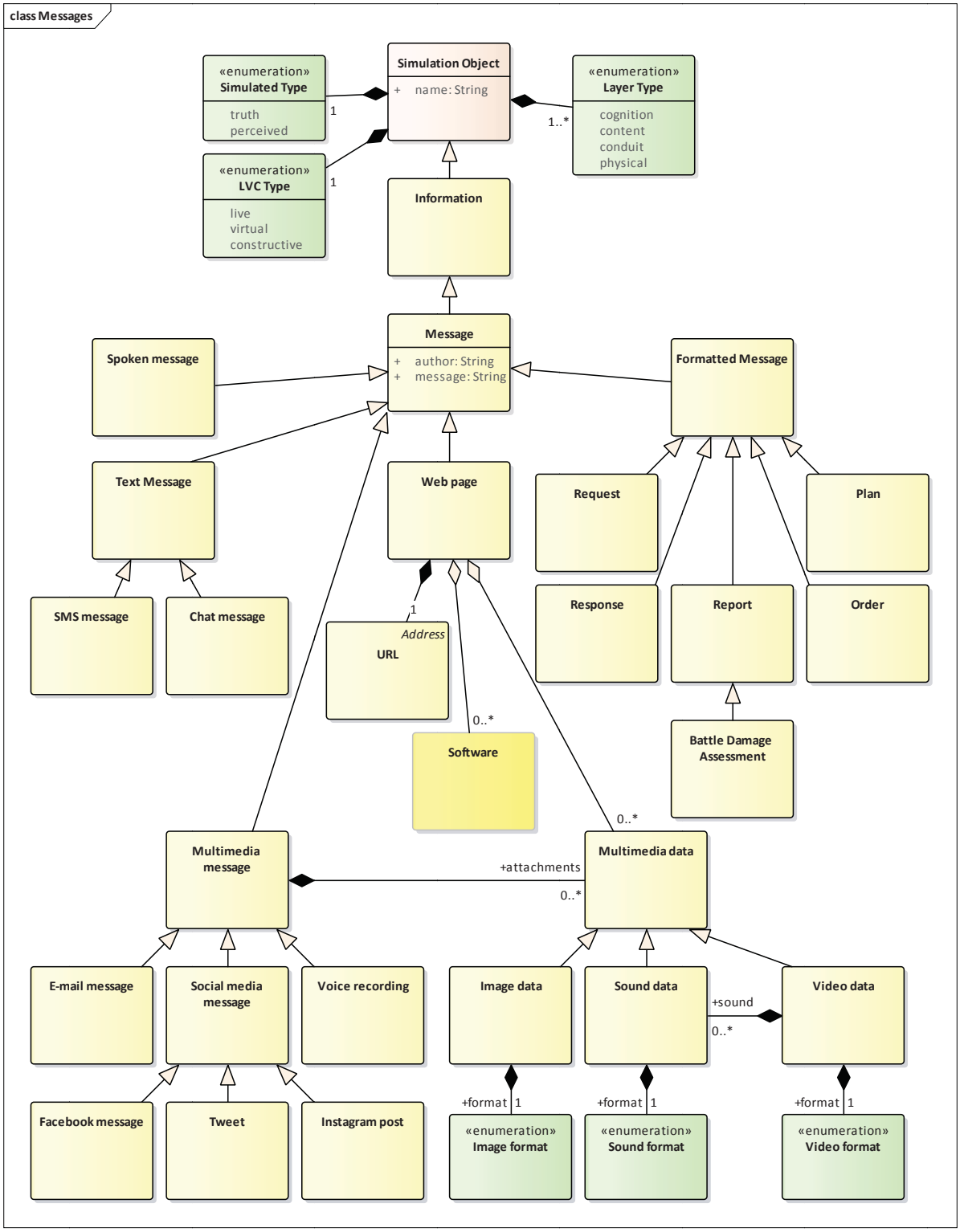

Figure 6-8: Class Diagram for the Message Object Classes of the IWSDM

6.3.3 Software Objects

Figure 6-9 shows a class diagram containing *Software* objects in the IWSDM. The *Software* class is a base class for all of the different types of software that may be modelled in the simulation, including operating systems, server software and end user (client) software. All software explicitly referenced in the Present OCO Simulation use case is represented. In addition, some that is not explicitly referenced, such as particular operating systems and office software, is also included in the diagram.

While objects of the classes shown in Figure 6-9 will be very commonly defined in the ORBAT and instantiated at simulation initialization time, it is also possible that some could be objects passed between components during simulation execution. For example, *Malware* software is transmitted between a website and cell phone during execution of the Present OCO Simulation use case.

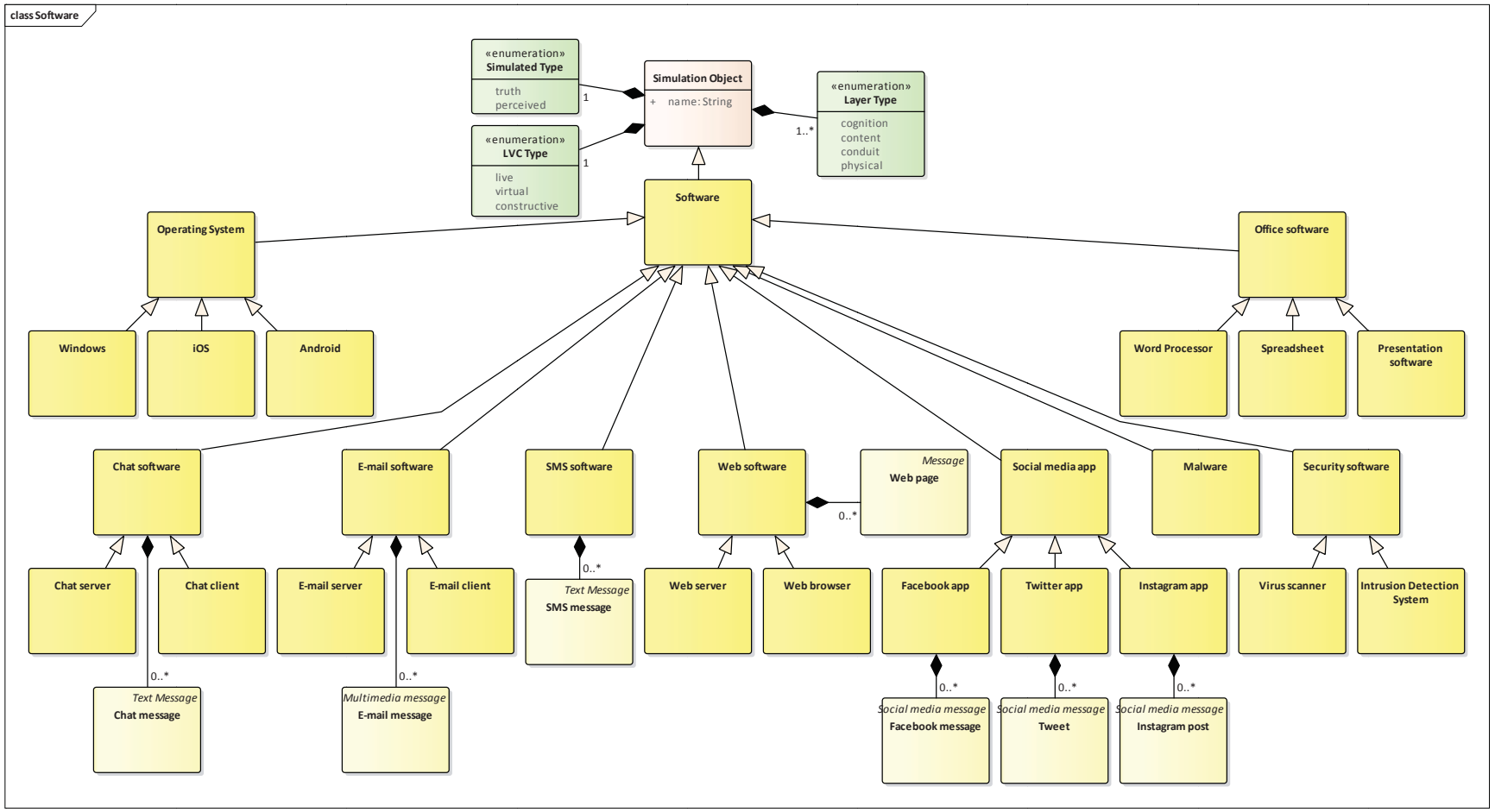

Figure 6-9: Class Diagram for the Software Object Classes of the IWSDM

6.3.4 Computing Equipment Objects

Figure 6-10 shows a class diagram containing computing equipment objects in the IWSDM. The *Data Processing Equipment* class is a base class for all of the different types of computer equipment that may be modelled in the simulation. The class hierarchy from *Material* to *Data Processing Equipment* and *Facility* to *Network* take their structure from the object hierarchy defined by the MIP Information Model (MIP, 2017).

For the Present OCO Simulation use case, we consider that the *Computer* and *Network interface* are the main classes that are derived from the *Data Processing Equipment* class. Other computing and network devices, including the *Laptop*, *Cell phone*, *Network gateway* and *Router* are assumed to extend the *Computer* and therefore have an *Operating System* and run *Software*. This makes them all more susceptible to multiple forms of Cyber attack than a simple hardware device.

The classes shown in Figure 6-10 are expected to primarily be defined in the ORBAT and instantiated at simulation initialization time.

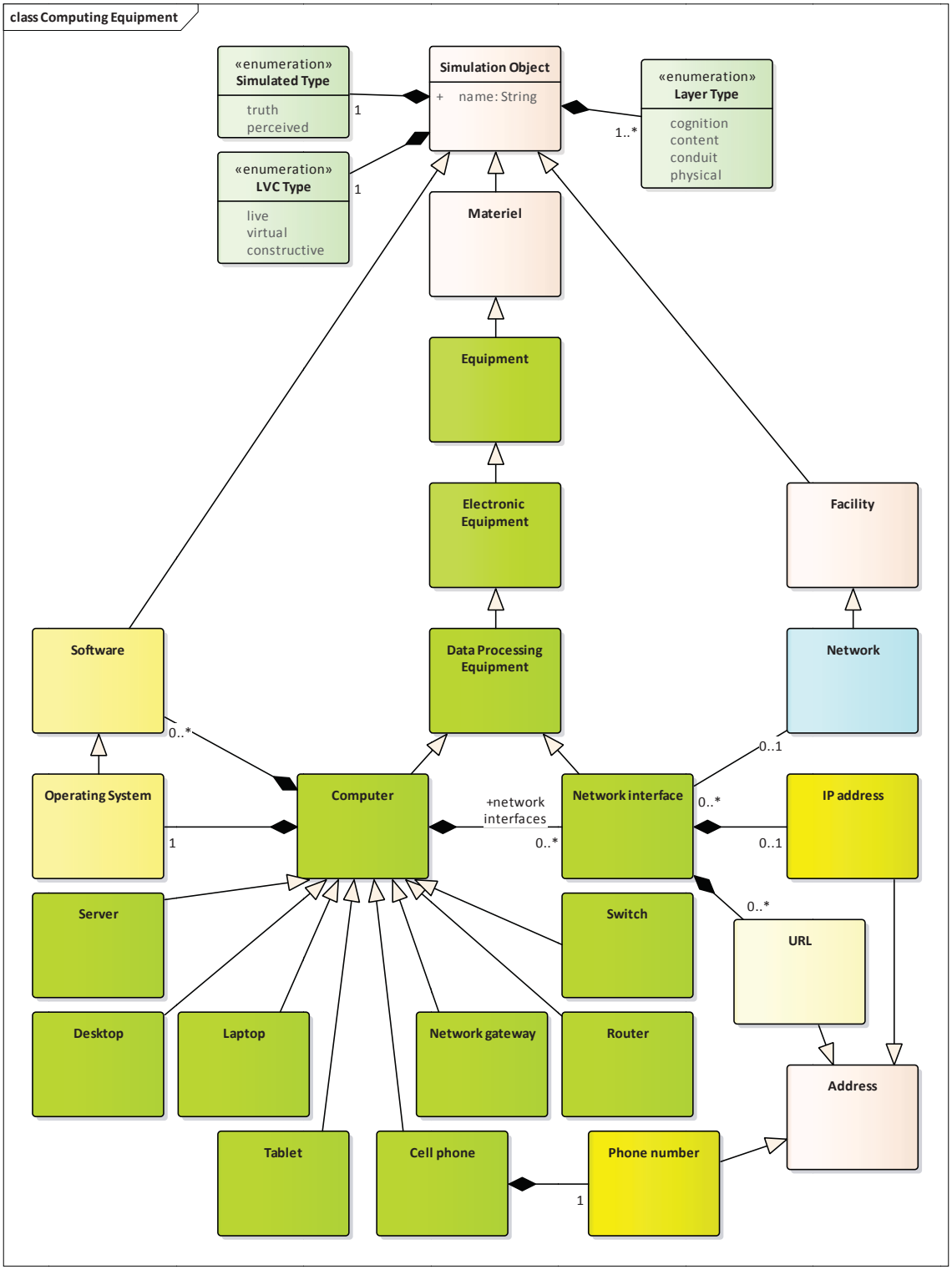

Figure 6-10: Class Diagram for the Computing Equipment Object Classes of the IWSDM

6.3.5 Network Objects

Figure 6-11 shows a class diagram containing *Network* objects in the IWSDM. The *Network* class is a base class for all of the different types of technology networks that may be modelled in the simulation. This includes computer networks, such as *LAN* and *WAN*, and communications networks such as *Cell phone network* and *Marine Radio network*.

The classes shown in Figure 6-11 are primarily expected to be defined in the ORBAT and instantiated at simulation initialization time.

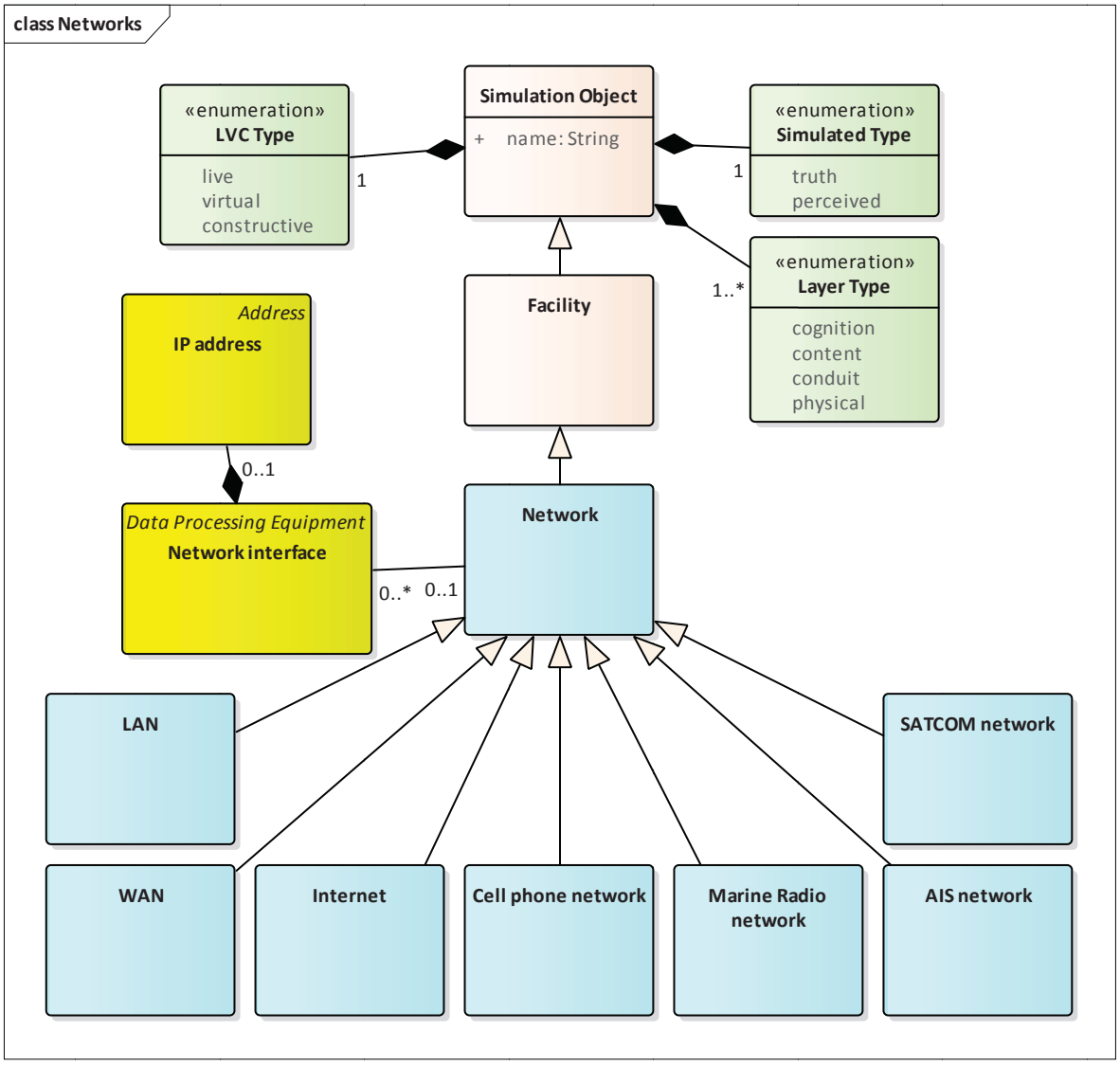

Figure 6-11: Class Diagram for the Network Object Classes of the IWSDM

6.3.6 Service Objects

Figure 6-12 shows a class diagram containing *Service* objects in the IWSDM. The *Service* class is a base class for all of the different types of technology services that may be modelled in primarily the Conduit layer but also the Content layer of the simulation for the Present OCO Simulation use case, such as e-mail services, cell phone services and web services. The *Service System* class is a base class for technology systems that implement the various technology services, such as software systems and cell phone service systems, while the *Service Provider Organization* class is a base class for the organizations that provide the various technology services, such as commercial ISPs and telecommunication companies. The class hierarchy from *Actor* to *Organization* take their structure from the object hierarchy defined by the MIP Information Model (MIP, 2017).

The classes shown in Figure 6-12 are primarily expected to be defined in the ORBAT and instantiated at simulation initialization time.

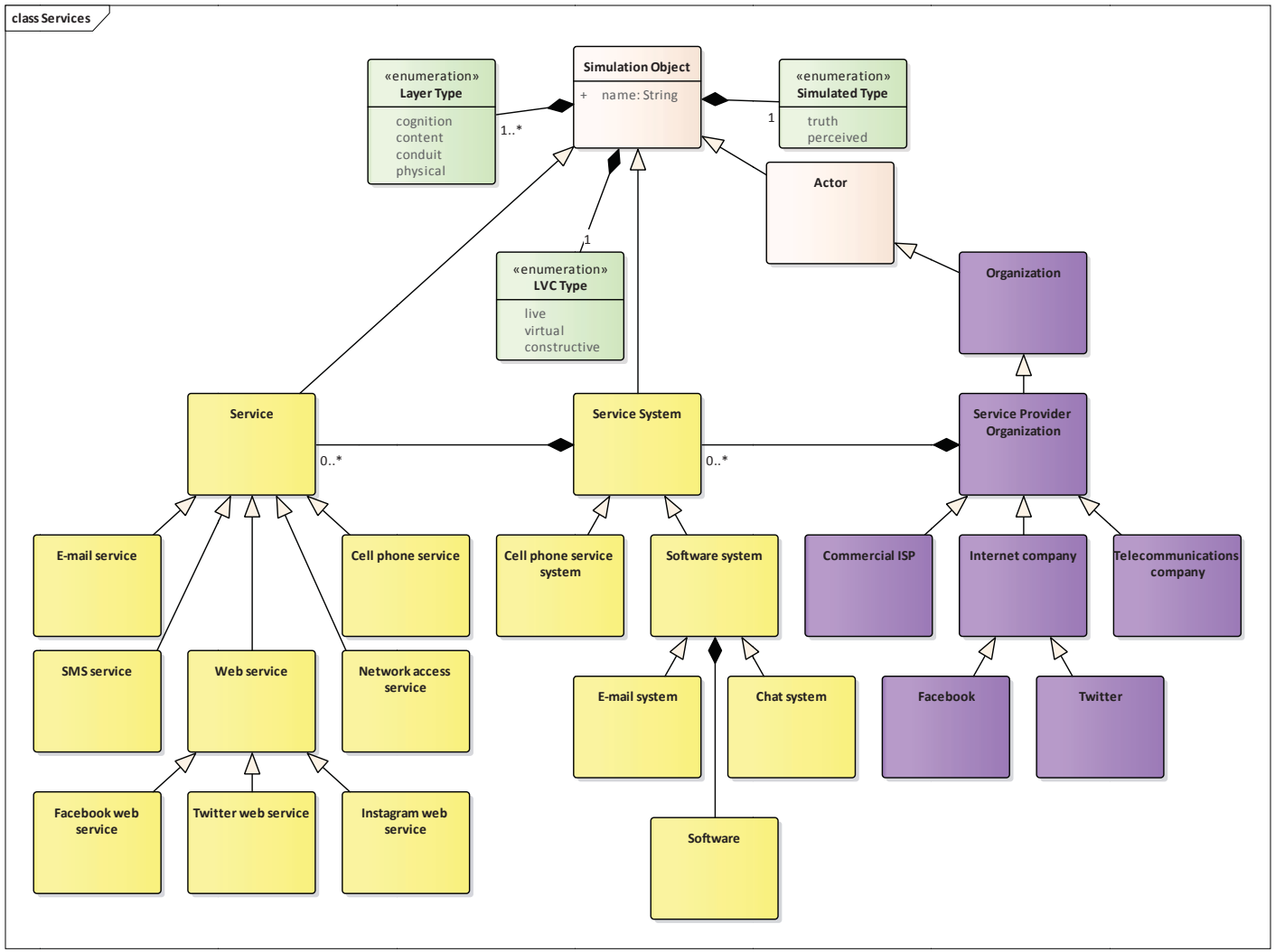

Figure 6-12: Class Diagram for the Service Object Classes of the IWSDM

6.3.7 Decision Maker Objects

Decision makers are important elements to include in an IWSDM because they represent components that are not widely supported in existing standardized simulation data models. As in previous sections, the scope of the current representation of decision makers, decision making procedures and the different types of cognitive data is bound by the elements defined explicitly in the Present OOC Simulation use case and is therefore intended to be both a framework and a start to defining a complete data model.

Figure 6-13 shows a class diagram containing *Decision Making* objects in the IWSDM. The *Decision Maker* class is a class that represents the decision makers that may be modelled in the Cognition layer of the simulation for the Present OOC Simulation use case. The *Decision maker procedures* class is a base class for the procedures used to make decisions by the *Decision Maker*. From a practical perspective, the class hierarchy headed by *Decision maker procedures* determines the capabilities of the decision makers in the Cognition layer. The *Cognitive data* class is a base class for the information that is a part of the Entity Internal Information that is modelled in the Content layer.

The decision maker classes shown in Figure 6-13 are primarily expected to be defined in the ORBAT and instantiated at simulation initialization time, while the cognitive data classes will be defined in the ORBAT and instantiated at simulation initialization time, and also used at run-time during simulation execution.

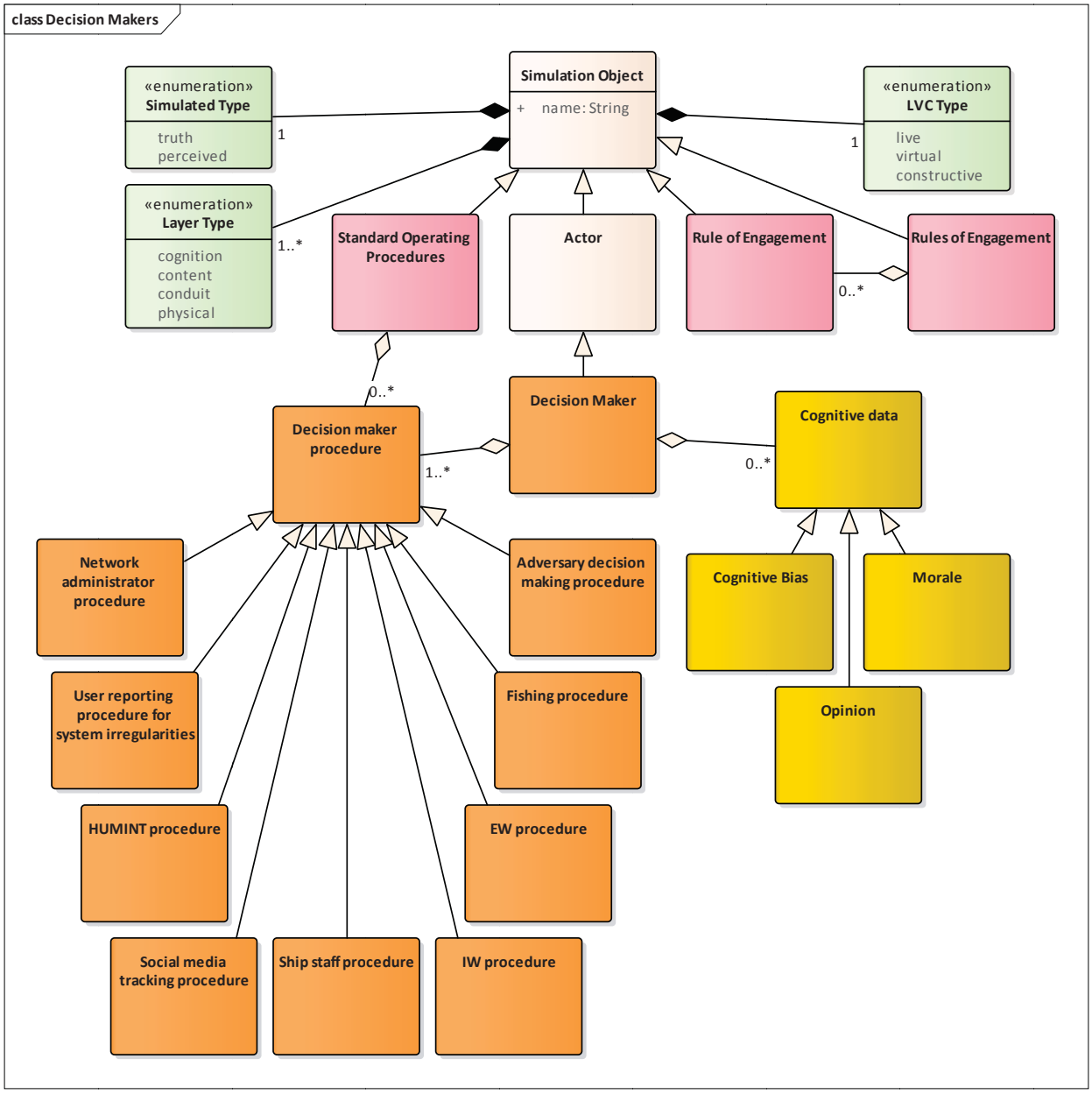

Figure 6-13: Class Diagram for the Decision Maker Object Classes of the IWSDM

6.3.8 Equipment Objects

Figure 6-14 shows a class diagram containing *Equipment* objects in the IWSDM that are modelled in the Physical layer of the IWSA. The internal (non-leaf) classes derived from the *Equipment* class, such as *Maritime Equipment*, *Electronic Equipment* and *Communication Equipment*, take their structure from the object hierarchy defined by the MIP Information Model (MIP, 2017), while each of the sensors, communications and electronic warfare equipment in

the Present OCO Simulation use case are represented in the diagram. Figure 6-14 also contains the *Track* and *Common Operating Picture* classes used by the sensors.

The classes shown in Figure 6-14 are primarily expected to be defined in the ORBAT and instantiated at simulation initialization time. In contrast, the *Track* and *Common Operating Picture* classes are used at run-time during simulation execution.

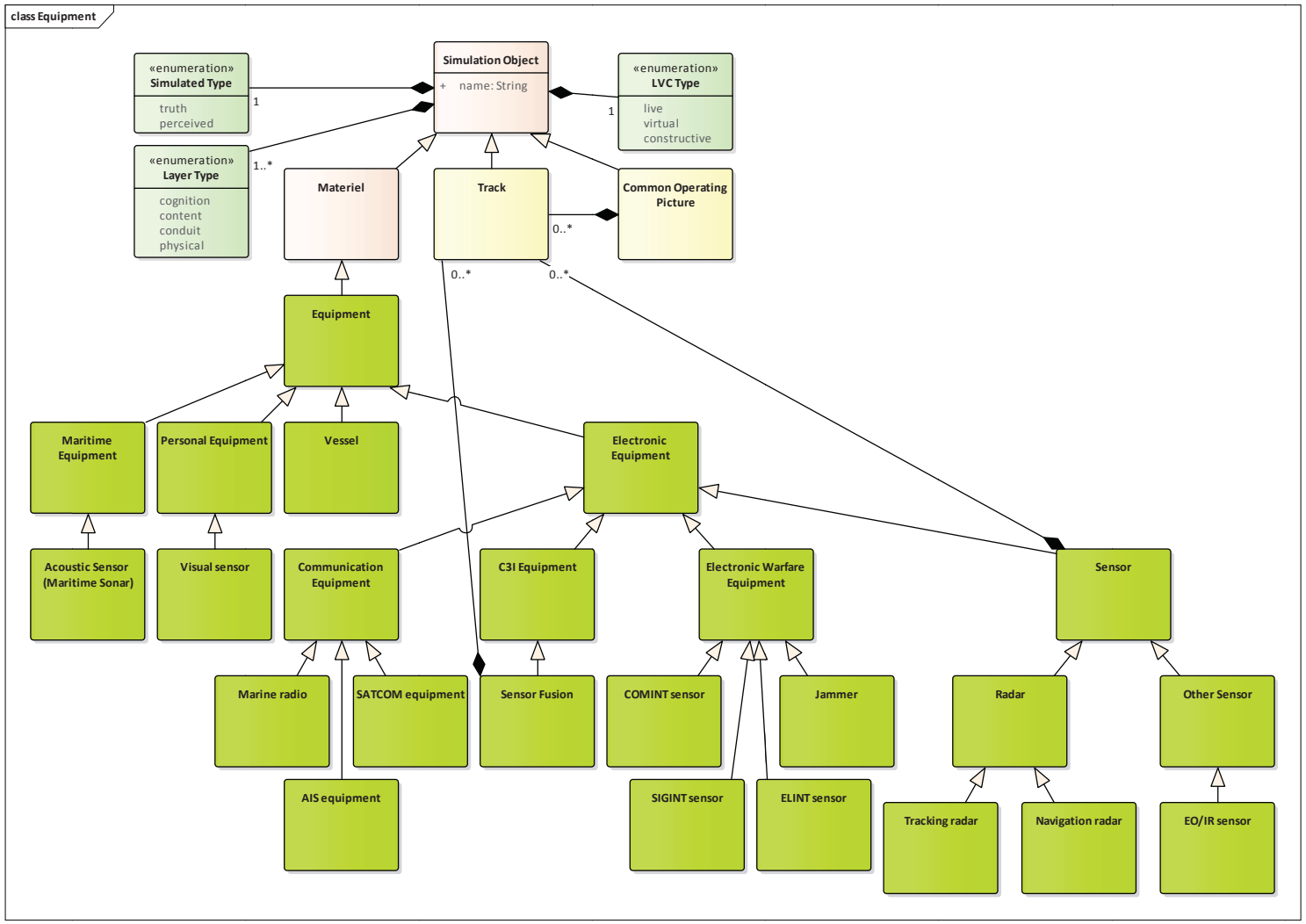

Figure 6-14: Class Diagram for the Equipment Object Classes of the IWSDM

6.3.9 Entity and Environment Objects

Figure 6-15 and Figure 6-16 shows class diagrams containing entity and environmental objects in the IWSDM that are modelled in the Physical layer of the IWSA. In these diagrams, the classes derived from the *Materiel*, *Actor*, *Feature* and *Organizational Structure* classes take their structure from the object hierarchy defined by the MIP Information Model (MIP, 2017). Each of the entity and environmental elements in the Present OCO Simulation use case are represented in these diagrams.

The classes shown in Figure 6-15 and Figure 6-16 are primarily expected to be defined in the ORBAT and instantiated at simulation initialization time.

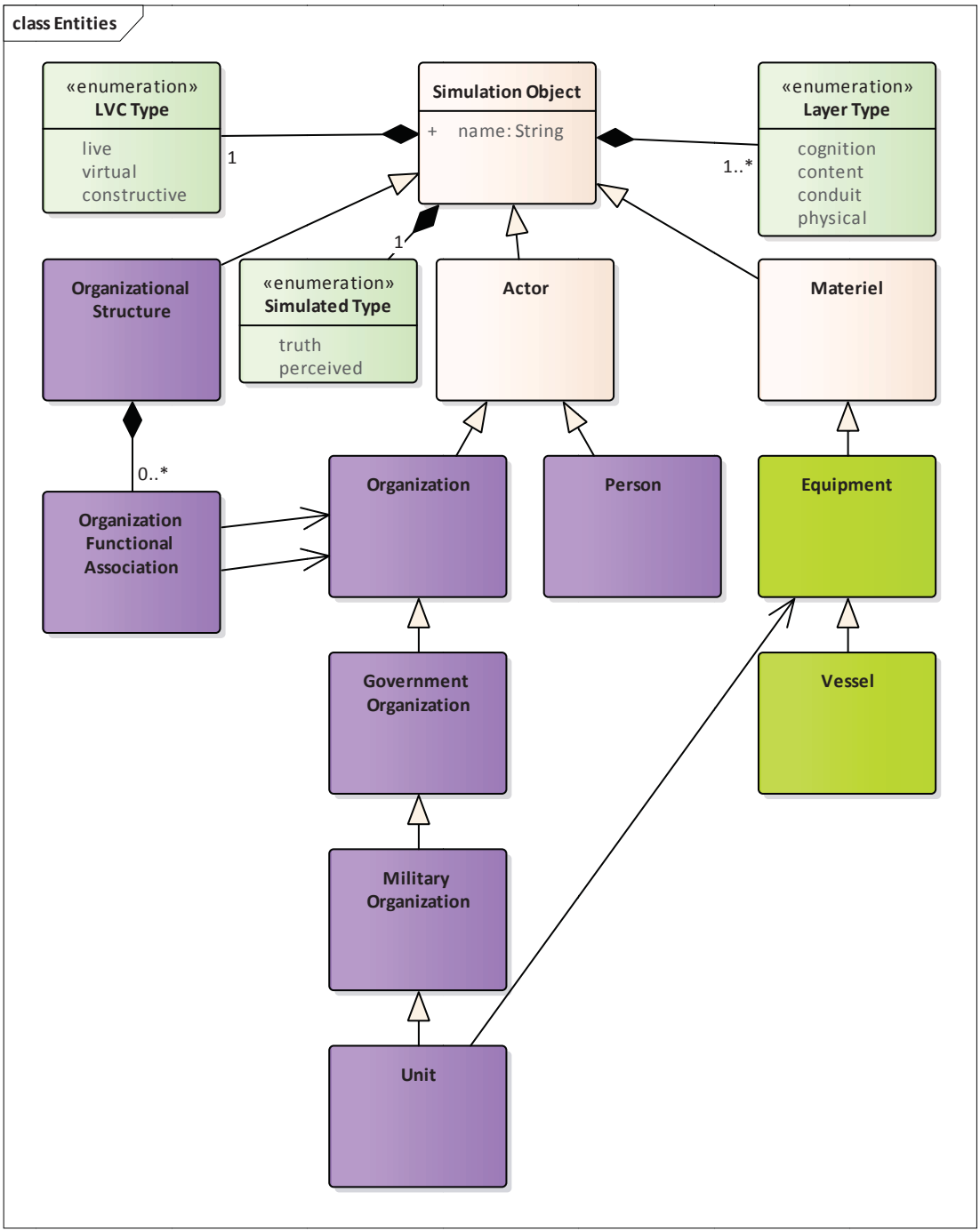

Figure 6-15: Class Diagram for the Entity Object Classes of the IWSDM

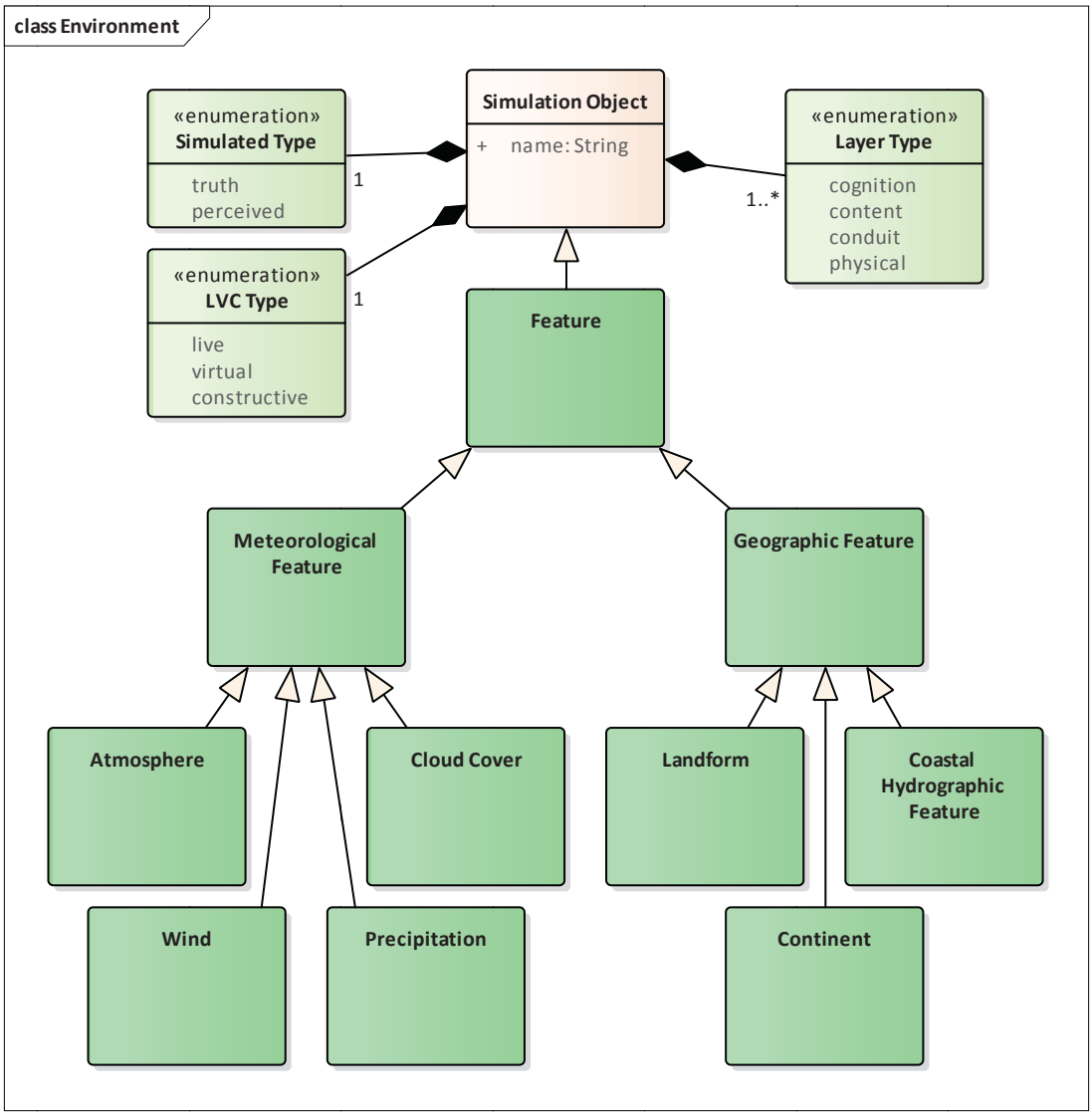

Figure 6-16: Class Diagram for the Environmental Object Classes of the IWSDM

6.3.10 Base Interactions

The *Interaction* is the base class for all interaction classes in the IWSDM, and is shown in the class diagram in Figure 6-17. All interaction classes are expected to be used at simulation execution time. While one would not normally expect the interaction classes to be included in the ORBAT or instantiated during simulation initialization, they could be used to represent a sequence of commands to be issued under certain conditions (such as a particular time) within the simulation and therefore it may be valuable to allow them to be included in the scenario specification ORBAT.

Figure 6-17 shows a number of interactions derived from the *Interaction* class, including interactions for dealing with Entity Internal Information in the Content layer. The *Status* class is expected to be the base class of many other classes, the *Communication Status* and *Sensor Status* classes shown in Figure 6-17are two of these. The *Information* and *Spoken message* classes are defined in Figure 6-8, while the *Track* class is defined in Figure 6-14. The *Command* interactions are described further in the next subsection.

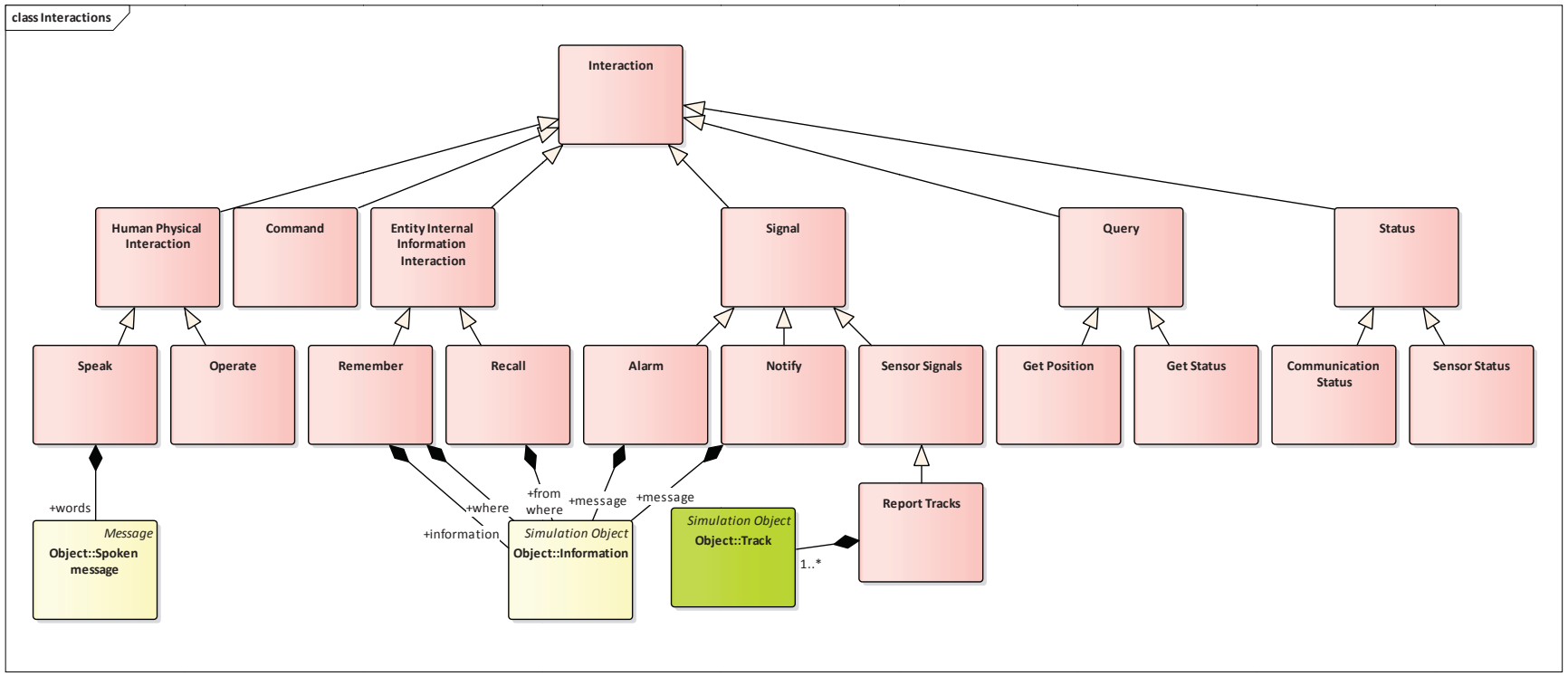

Figure 6-17: Class Diagram for Basic Interaction Classes of the IWSDM

6.3.11 Command Interactions

Figure 6-18 shows a class diagram containing *Command* interactions in the IWSDM. The *Command* class is a base class for all of the different types of commands affecting any of the elements in the IWSA. Each of the interactions in Figure 6-18 that derive from *Command* are implied by the Present OCO Simulation use case. Note that the class hierarchies derived from the *Equipment Command* interactions follow a similar structure to the *Equipment* object classes shown in Figure 6-14.

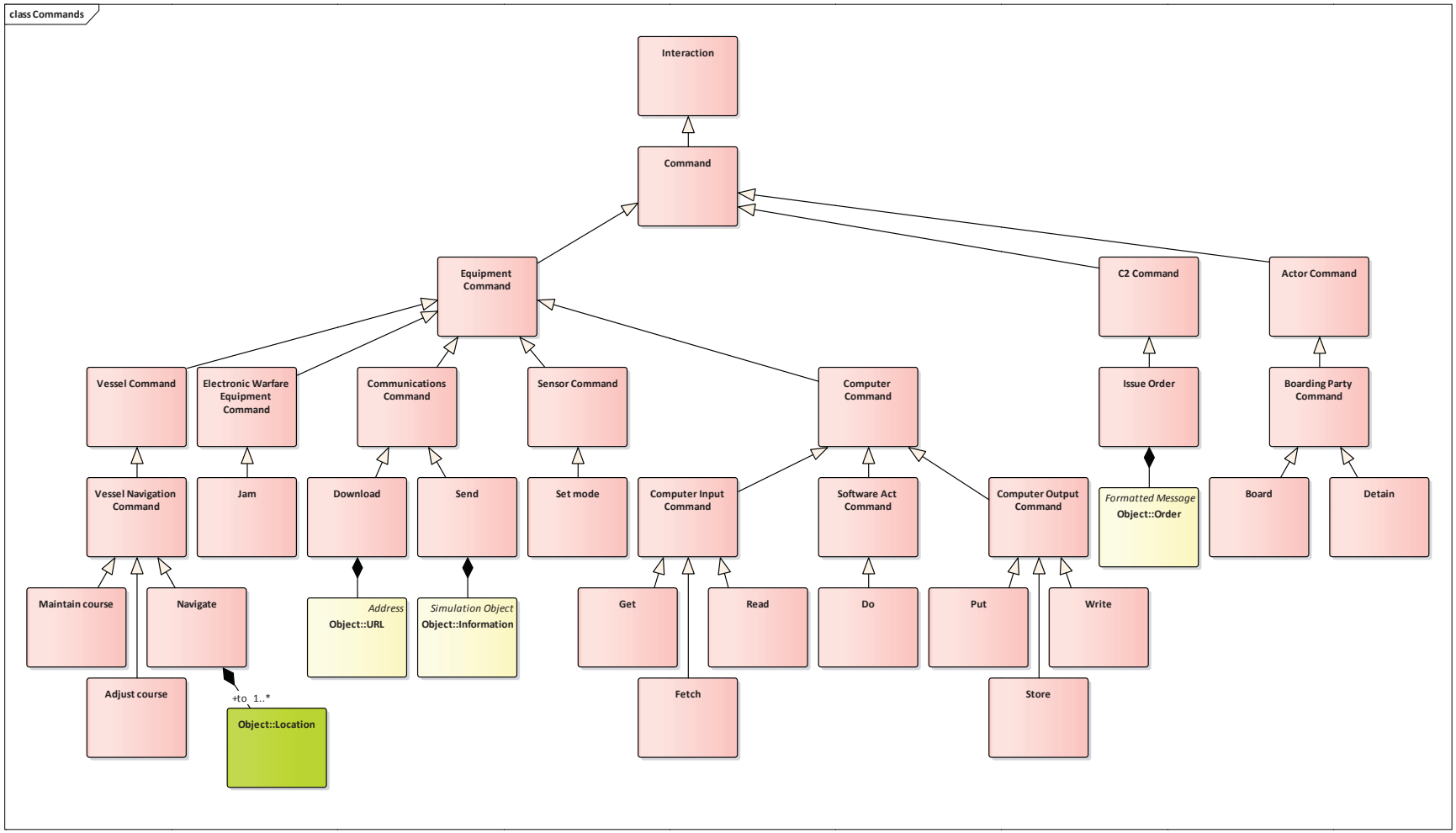

Figure 6-18: Class Diagram for Command Interaction Classes of the IWSDM

6.4 Comparison with Other Data Models

6.4.1 MIP Information Model

The Multilateral Information Programme (MIP) is a standardization body that is developing the MIP Information Model (MIM) (MIP, 2017) 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) (MIP, 2012).

The primary focus of the MIM is not simulation, although the elements within the data model could be simulated and components using the MIM could be involved in a live simulation. However, it does not represent a complete data model from a simulation perspective.

When considering the IWSA, the MIM defines classes that belong in the Physical, Conduit and Content layers, although the representation is not complete from the perspective of the IWSA. The MIM includes a representation of computer and communications hardware, networks and some network services. It also includes classes for plans, orders and reports. As its focus is C2, 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.

To the best of our knowledge, neither the JC3IEDM nor the MIM are widely supported by existing CGFs.

6.4.2 C-BML, MSDL and C2SIM

The Coalition Battle Management Language (C-BML) (SISO, 2014) is a language designed to support the exchange of plans, orders, requests and reports across C2 and LVC M&S systems. Its data model is based on, and is an extension of, JC3IEDM. As such, as in the case of MIM, the successor to JC3IEDM, C-BML defines classes that belong in the Physical, Conduit and Content layers, although the representation is not complete from the perspective of the IWSA. Similar to the MIM, it does not include a representation of decision makers, decision making processes, or how some services in the Content and Conduit layer may be implemented.

The Military Scenario Definition Language (MSDL) (SISO, 2015) is a language designed to support the development of scenarios (e.g., ORBATs) that can be 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 the IWSDM defined in section 6.3 because it defines elements that belong to the Physical and, to a lesser extent, the Conduit layer and does not consider 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 which belongs in the Content layer.

There is an effort currently underway within Simulation Interoperability Standards Organisation (SISO) to effectively merge C-BML and MSDL to create a standard for Command and Control

Systems – Simulation Systems Interoperation (C2SIM) (SISO, 2017). It would be advantageous for the new standard to be extended to support additional elements from the IWSA and IWSDM.

6.4.3 DIS PDUs & HLA RPR FOM

The data model defined by the Distributed Interactive Simulation (DIS) Protocol Data Unit (PDU) standard, originally defined in (IEEE, 1995) and amended in (IEEE, 1998) (referred to as DIS 6), and the equivalent representation for the High Level Architecture (HLA) – the Real-time Platform Reference (RPR) Federation Object Model (FOM) – defined in (SISO, 2015), 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 initialization.

The DIS 6 PDUs and HLA RPR FOM are largely complementary to the IWSDM defined in Section 6.3 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. At the Conduit layer, the PDUs focus is on transmissions and emissions rather than transporting content. In contrast, the IWSDM concentrates in more detail on the Content and Cognitive layers. DIS 6 also includes simulation management PDUs, for management of simulation applications rather than simulation content, that we have not currently included in the IWSDM.

The most recent revision of the DIS standard (IEEE, 2012) (DIS 7) added additional PDUs for Information Operations (IO): the IO Action PDU and IO Report PDU. The IO Action PDU is used to communicate an IO attack or the (predicted) effects of an IO attack on targets. The IO Report PDU is used to communicate the (actual) effects of an IO attack on targets. While the intent of the 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 IWSA. To the best of our knowledge, these IO PDUs are not widely supported by existing CGFs.

7 DISCUSSION AND RECOMMENDATIONS

7.1 Analysis Status

In our analysis of the use case, we chose to perform a top-down decomposition of the domain. 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.

We documented the use case using two different representations. At the summary level, we used Cockburn's fully dressed form (Cockburn, 2000) with the addition of a story to provide a guiding narrative. This proved effective at encapsulating the use case so that the intent and scope could be understood. At a more detailed level, we used a sequence of numbered steps as suggested by Fowler (Fowler, 1999). This representation proved to be particularly useful for structuring the analysis of the operational systems and activities, and consequently deriving communication diagrams. As such, for analysis of future use cases we believe that both summary level and more detailed steps are valuable.

From an object-oriented design point of view, our analysis shows that many objects/entities in our data model 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, to 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 (be the responsibility of) different services provided by a range of layers. For example, the human entity's physical location attribute is the responsibility of services instantiated by objects derived from the *Actor* object in the physical layer, while the internal content is in the content layer and the cognition in the cognitive layer.

Throughout the analysis, we believed that it was 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.

7.2 CGF Implementation Considerations

Whilst current CGF systems offer the opportunity to develop internal low fidelity information warfare effects, the IWSA shown in Figure 4-2 provides a framework to develop and federate services representing higher (and differing) fidelities of IW effects to match the requirements of different 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.

Designing future simulation systems incorporating modern design principles implies the use of common modular re-useable services. Systems so developed will be aligned with the future anticipated delivery of Simulation-as-a-Service (SaaS) environments. A range of tools and common services could then be developed, such as an EW Service, Cyber Service, Network Emulation Service, and Behaviour Modelling Service.

In this service oriented architecture (SOA) design each layer would have the ability to contain multiple services providing different fidelities or elements. 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).

The cost of this increased complexity will be in the increased amount of configuration and background data required to setup and run scenarios. Verification and validation (V&V), analysis and after-action review activities using data logged from simulation are required, and are likely to be equally complex. Simulation systems need to be designed to output IW data to facilitate these activities. 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.

7.3 Recommendations for Future Work

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, in which case it may be necessary. 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, biases and cognition layer interactions, 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 IWSA that are not yet covered in sufficient detail or generality are primarily the upper layers of the architecture: the content and cognition layers. 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 cognition layer are not covered well by existing simulation products or standards. This should include identifying additional patterns that apply to interfaces and interactions between components in these layers.

All areas of IW effects can benefit from additional research. Psychological operations are the least well defined and it is likely that significant progress will be 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) 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 explore the engineering issues raised in greater depth.

In the longer term, we believe that additional use cases and implementations must be explored for different applications (for example, analysis as well as training) and in different domains (other maritime, air, land and joint) prior to standardising a data model, either as an extension of an existing data model or by developing a new one.

7.4 Conclusion

The work reported here is the first step in validating the IWSA following a use case based approach. Compared to previous work (Hazen, Lloyd, & Harris, The Evolution of Computer Generated Forces (CGF) Architectures to Support Information Warfare Effects, 2016), 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, but has not identified any major flaws in the IWSA. As such, the use case analysis process we described should provide a good initial structure for further investigation of the architecture.

In documenting the use case, we found it to be valuable to supplement the fully dressed use case form of Cockburn with a narrative (story) to provide an overall structure and guidance for the use case, while also decomposing it to a step-by-step walkthrough of the scenario to expose the details required for our analysis.

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

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Atlantic Research Centre
Defence Research and Development Canada
9 Grove Street
P.O. Box 1012
Dartmouth, Nova Scotia B2Y 3Z7
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Information Warfare Simulation Architecture Development: Task Report

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to beused)

Harris, E.; Lamoureux, T.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
November 2017	152	34

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Atlantic Research Centre
Defence Research and Development Canada
9 Grove Street
P.O. Box 1012
Dartmouth, Nova Scotia B2Y 3Z7
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
	W7719-155268/001/TOR Task12

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2017-C278	01DB

11a. FUTURE DISTRIBUTION (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Any limitations on further dissemination of the document, other than those imposed by security classification.)

12. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

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. This contract report contains the result of a systems engineering analysis of the simulation architecture. 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. The analysis did not find any structural issues with the simulation architecture, but did find major gaps in current simulation data models with respect to the representation of content and cognitive layer data structures. The analysis also noted the requirement for the separation of simulation truth and perceived data, and the fact that some traditional simulation objects (e.g. military units) have characteristics found in all four levels of the architecture.

L'espace de combat est souvent dépeint comme un ensemble de couches présentant différents aspects qui vont du terrain aux flux d'information. Les simulations de forces générées par ordinateur utilisées lors de campagnes ou de missions sont généralement axées sur la représentation physique des unités, du terrain et des effets. En 2016, on a proposé une architecture de simulation en couches pour orienter l'évolution des forces générées par ordinateur afin d'inclure les effets de la guerre de l'information. Ce rapport de contrat présente le résultat d'une analyse technique des systèmes de l'architecture de simulation. On a précisé davantage la description de l'architecture de simulation pour faciliter l'instruction collective des officiers d'état-major de la Marine sur la guerre de l'information. On a rédigé des descriptions détaillées du contenu et de la capacité de couche, ainsi que des flux de données intra-couches et inter-couches. À partir de ces descriptions, on a élaboré un modèle initial de données pour faciliter l'analyse de l'utilité des modèles actuels de données d'interopérabilité pour cette application. Ce travail pose les bases de la description d'une architecture commune des composants de simulation requis en vue de modéliser les effets de la guerre de l'information. L'analyse n'a révélé aucun problème de nature structurelle dans l'architecture de simulation, mais a permis de déceler des lacunes importantes dans les modèles actuels de données de simulation quant à la représentation du contenu et des structures de données des couches cognitives. L'analyse a aussi permis de souligner la nécessité d'une séparation de la vérité de la simulation et des données perçues, de même que le fait que certains objets traditionnels de la simulation (p. ex., unités militaires) possèdent des caractéristiques qu'on peut retrouver dans les quatre niveaux de l'architecture.

13. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

information warfare; simulation; architecture;