Experimental Evaluation of a Command and Control – Simulation Interoperation Standard in a Coalition Environment

J. Mark Pullen
C4I & Cyber Center George Mason University
4400 University Drive
Fairfax, VA 22030, USA
mpullen@c4i.gmu.edu

Brian Wardman
Defence Science and Technology Laboratory, UK Ministry of Defence
Portsdown West, Portsdown Hill Road
Fareham, Hants, UK PO17 6AD
bwardman@dstl.gov.uk

James Ruth
Trideum Corporation
1000 S. 4th Street, Suite C
Leavenworth KS 66048, USA
jruth@trideum.com

Keywords: interoperability standard, experimental technology evaluation, coalition command and control-simulation

Abstract

The NATO Modelling and Simulation Group (MSG) Technical Activity 145 and SISO Product Development Group for the C2-Simulation Interoperation (C2SIM) have been working together to standardize and operationalize a new capability, which has been described in previous ICCRTS papers by the authors. SISO anticipates balloting the standard late in 2019. This paper reports on an experimental evaluation of the new C2SIM standard that has been undertaken by MSG-145 in preparation for the balloting process. The paper describes the experiment design and its rationale, and includes experimental results.

The planned evaluation involves experimental application of systems that implement the SISO draft C2SIM standard. Software systems from France, Germany, Italy, New Zealand, the UK and the USA interoperated. Evaluation was performed in phases, over a three-month period:

- Experimental application done independently by six national teams, exploring use cases they have been developing since the beginning of MSG-145. A corollary benefit of this phase is that the implementations have been confirmed as operational and the users familiar with them.
- Detailed validation testing of all information flows in the coalition of C2SIM systems in conjunction with NATO Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXcercise (CWIX) 2019, via an Internet Virtual Private Network (VPN).
- Experimental use in a small-scale coalition military distributed mission planning exercise. This includes experimental evaluation of the cyber emulation capability described in a 2018 ICCRTS paper.

1. C2SIM Overview

The ability to interoperate command and control (C2 or mission command) systems with simulation systems has been an important goal for more than a decade [1]. Over that period, the NATO Modelling and Simulation Group (NMSG) has been cooperating with the Simulation Interoperability Standards Organization (SISO) to develop, prototype, and test standards that support that capability. The vision is that members of a coalition will be able to combine their C2 systems and simulation systems collectively into a system-of-systems where simulations are tasked by the C2 systems and, in turn, provide reports that are displayed on the C2 system just as they would appear due to real- world operations. The resulting system of systems can support training, course of action analysis, and mission rehearsal for the coalition. Each force element uses the C2 system with which it has trained and is represented by a simulation that represents well its doctrine, resources, and tactics/techniques/procedures. Sharing information this way will result in more effective, rapid coalition operations [2].

Standards enabling the vision described above are well along in development by SISO and may reach the balloting phase by the end of 2019. In order to finalize effective standards, the NATO Technical Activity MSG-145 *Operationalization of Command and Control – Simulation Interoperation* (C2SIM) undertook a validation process. This paper describes that process, beginning with the roles and motivations of NATO and SISO, then providing background on C2SIM. After that we consider the activities of the eight national teams involved and then explain how they enabled validation of C2SIM through a coordinated effort that provided compliant interfaces on six different simulations and one C2 system and also supporting software. The validation effort took these C2SIM-enabled systems to the NATO CWIX for detailed testing and then culminated with experimentation, structured as a miniature exercise in distributed mission planning. The paper concludes with lessons learned from the validation process and a view toward the future of C2SIM-based coalition interoperability.

2. NATO and SISO Roles Developing C2SIM

The mutually supporting partnership between MSG-145 and the SISO C2SIM Product Development Group (PDG) has been essential in reaching a point where C2SIM can be validated, and even more critical in the validation process. As a collaborative organization of industry, academic and government representatives, SISO does not have the ability to develop working prototype systems-of-systems or to validate them with international military participation. Conversely, NATO is not in a position to develop industry- based standards. Complementary, cooperative work between the two has been needed to create the C2SIM standard.

MSG-145 is the third in a sequence of NATO Technical Activities that has supported development of C2SIM. The first, MSG-048 *Coalition Battle Management Language*, completed validation of the technical feasibility of coalition C2-simulation interoperation. The second, MS-085 *Standardization for C2-Simulation Interoperation* supported and tested the first generation of C2-simulation interoperation standards: *Military Scenario Definition Language (MSDL)* [3] and *Coalition Battle Management Language (C-BML)* [4]. A key outcome of MSG-085 was a determination that, while MSDL and C-BML can be made to work together, a second generation standard was needed to achieve effective harmonization; also that the second generation should be designed for extensibility [5]. SISO responded by forming a merged PDG with a charter to achieve these objectives under the unified name C2SIM [6]. A goal of MSG-145 is to recommend and support a NATO Standardization Agreement (STANAG) based on the C2SIM industry standard.

SISO's activities to create C2SIM have been based on a complete bottom-up review of both C-BML and MSDL with a view to the result serving as the basis for a family of extensions. The C2SIM PDG concluded that the best way to approach this was developing a consistent family of ontologies. Development has been underway since 2014 and recently produced a set of draft ontologies that is ready for implementation, along with an approach to extracting a standard XML schema from the ontologies to support implementation for validation.

3. C2SIM Technical Description

Figure 1 shows the general architecture of a C2SIM coalition. The C2 systems interoperate using a C2 standard; the simulation systems interoperate using a simulation standard; and the system of systems interoperates using C2SIM. A web service is used to replicate C2SIM messages for distribution among the constituent systems and to produce a log that documents results of the operation.

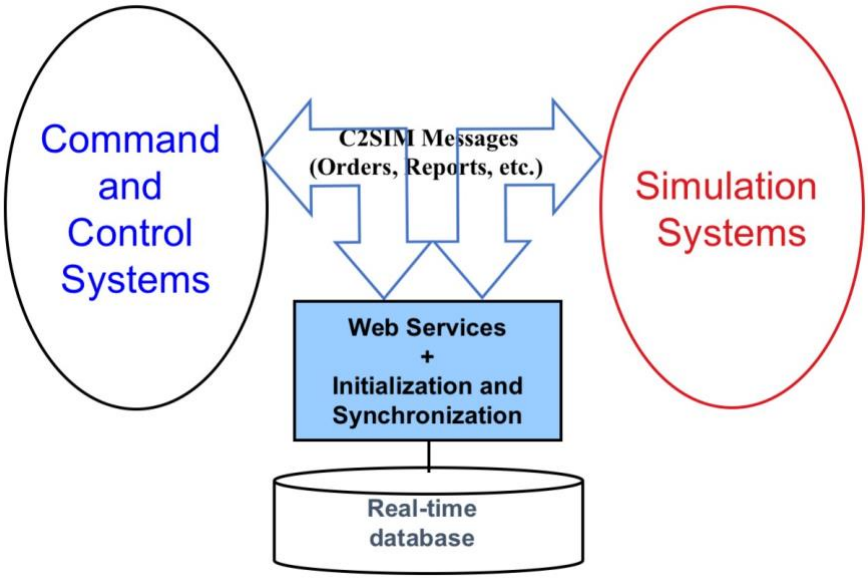

Figure 1: C2SIM Coalition General Architecture

The draft C2SIM standard consists of a text document defining rules and procedures for interoperation and for maintenance of the ontologies; a Core ontology consisting of data classes expected to be needed by any operational simulation; a Standard Military Extension (SMX) with classes applicable to all domains of military activity; and a Land Operations Extension (LOX) to encompass the capability originally provided by MSDL and C-BML and also to serve as an exemplar for future extensions. SMX is logically part of the main C2SIM standard, while LOX forms a new layer over Core+SMX.

The main text standard document is organized into the following sections:

1. Overview
2. References
3. Definitions, Acronyms, and Abbreviations
4. Compliance Strategy for the C2SIM Standards Set

5. Description of C2SIM Ontologies (this is supplemented by the ontologies themselves, which are "normative" (required for compliance) and also by an extracted text overview of each ontology
6. Extending the Logical Data Model
7. Initialization Procedures
8. FIPA-derived Procedures (C2SIM embraces the IEEE FIPA Agent Communication Language standard to ensure effective communication)
9. Message Processing
10. Maintenance of the C2SIM Ontologies

Appendix A: Data Format Definitions
Appendix B: C2SIM Ontology to XML Schema Definition Procedure

Other documents comprising the C2SIM standards are:

- C2SIM Core Ontology
- C2SIM Standard Military Extension Ontology
- C2SIM Guidance Document providing non-normative information to aid implementation
- Land Operations Extension to C2SIM
- Land Operations Extension Ontology

An important aspect of the C2SIM standard is maintenance of the ontologies. The C2SIM PDG envisions these as living documents that will evolve over time, as the user/implementer community embraces C2SIM and refines the data definitions in the ontologies. The use of ontologies provides a more dynamic and flexible tool for C2SIM users. The draft C2SIM standard calls for a process conducted by the SISO Product Support Group (PSG) that will take over from the PDG after balloting: a new, numbered ontology version can be approved by a heavy majority vote of the PSG. For implementation, all applicable ontologies are aggregated and the resulting composite ontology is transformed into an XML schema format for ingestion into user systems by a standard process.

4. Independent development of C2SIM interfaces by MSG-145 national teams

The first step in the C2SIM validation process was to add C2SIM interfaces to C2 and simulation software systems. During the period January to May 2019, several of the national teams that participate in MSG-145 did this, as described below. Most nations tested their implementation in the context of a use case it had focused on as part of MSG-145.

France: the French company MASA developed a C2SIM interface for their SWORD military simulation

Germany: the German company iABG developed a C2SIM interface for their KORA military simulation, related to their focus use cases *unmanned autonomous systems* and *army command post training*

Italy: Italy has the lead role in the NATO Modelling and Simulation Centre of Excellence (MSCOE); they sponsored development of a C2SIM interfaces for two simulations, expanded for their focus use cases to include an experimental *Autonomous Systems Extension* (ASX): (1) MAK's commercial military simulation VRForces and (2) the MASA Sword system

New Zealand: the Defense Technology Agency of New Zealand developed a C2SIM interface for the VBS3 military simulation, consistent with their focus user case *maritime operations*

United Kingdom: developed a C2SIM initialization and tasking interface for the Joint Semi-Automated Forces (JSAF) military simulation; for reports they continued to use the IBML09 interface from previous years, which was not a problem since the server used features a legacy interface that translates between IBML09 and C2SIM; their focus use case was *noncombatant evacuation operations*

USA: George Mason University (GMU) C4I and Cyber Center has developed the C2SIM Sandbox, consisting of the open source C2SIM Reference Implementation Server, the open source BMLC2GUI editor (which can serve as limited surrogate C2 system) and an open source C2SIM interface module for the MAK commercial military simulation VRForces; they updated all of these to the C2SIMv9 standard draft and also created a C2SIM interface module for the commercial C2 system SitaWare that was adopted recently by the US Army. The server is capable of supporting experimental modification of C2SIM messages to impose cyber effects, consistent with GMU's focus on operational training in cyber-active environments [7]. Trideum Corporation adapted the US Army simulation OneSAF to C2SIM, supporting the Army Test and Evaluation Command (ATEC). Unlike the C2SIM Sandbox software, the SitAware and OneSAF interfaces are not available as open source.

5. CWIX Testing for Validation

The NATO CWIX is an annual event, based at the Joint Forces Training Center (JFTC) in Bydogszcz, Poland, and extended worldwide through the classified Combined Federated Battle Laboratories Network (CFBLNet) and the unclassified Internet. CWIX focuses strongly on highly structured testing of systems that claim to be interoperable [8].

C2SIM Validation testing in CWIX 2019 was conducted using virtual private networks (VPNs) over the unclassified Internet. The national teams that participated in C2SIM Validation testing, the systems they used, and their locations were:

Germany: KORA and BMLC2GUI at JFTC, Bydgoszcz Poland

Italy: VRForces, SWORD and BMLC2GUI at MSCOE, Rome Italy

United Kingdom: JSAF and BMLC2GUI at Defence Science and Technology Laboratory (DSTL), Portsdown UK

USA Site 1: OneSAF, SitAware (reports only) and BMLC2GUI at ATEC, Huntsville Alabama

USA Site 2: VRForces, SitAware (reports only) and BMLC2GUI at Naval Postgraduate School (NPS), Monterey California

Server sites: for Europe at MSCOE, Rome Italy linked to USA at GMU, Fairfax Virginia

Monitor Site: BMLC2GUI at JFTC

Figure 2 shows the network architecture for C2SIM Validation in CWIX 2019. The bifurcation of networks with one VPN operated by the MSCOE and the other operated by GMU was necessary to meet the condition that SitAware and OneSAF software could not be on a network reachable by non-USA participants. There was one server on each VPN, operating as linked servers [9] through a firewall that allowed only the C2SIM ports to connect, which met both policy and technical requirements.

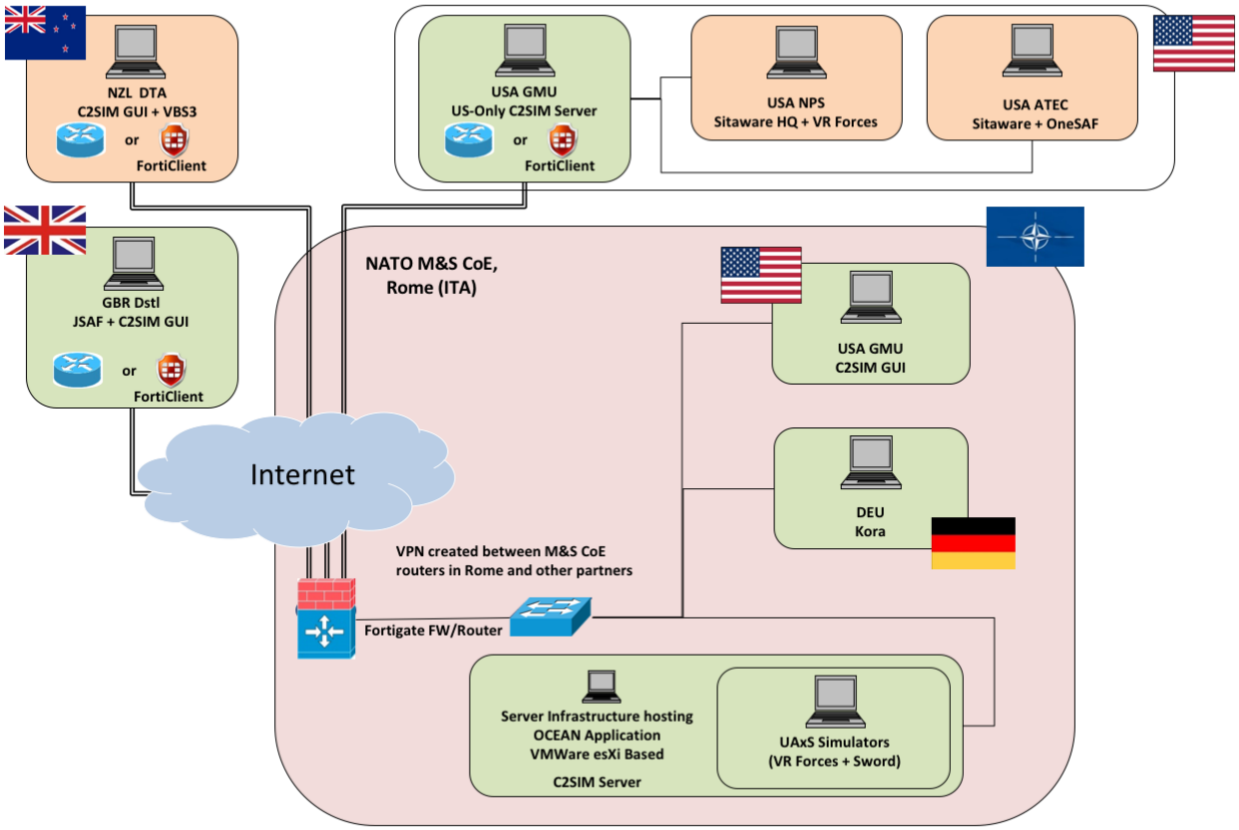

Figure 2: C2SIM Validation Network Architecture for CWIX 2019

Coordination for the CWIX testing was provided by the commercial Internet conferencing tool Zoom, which provided all the functionality needed, including voice, text chat, and screen sharing. It operated outside of the VPN in order that its client could connect to the Zoom server.

C2SIM Tests were documented through the CWIX Wiki as required by the methodology of CWIX. They were conducted by the coalition of national teams listed above are shown in Table 1. Tests were reported by each site, with the two USA sites contributing to a single report for CWIX purposes because as remote sites under the same nation they were considered a single “capability”. The first four tests were scheduled for the first day of testing, the next two were scheduled for the second day, and the final two (Cyber Electronic Warfare (EW) effects) were scheduled for the last day. This schedule was maintained, with exceptions caused by system problems at sites in the UK and USA which caused the first four tests to be delayed to the second day. Each site reported success, limited success, or failure for each group of tests (1, 2 and 3), giving a total of twelve Test Cases for the C2SIM Validation coalition.

At the end of testing, eleven of the twelve Test Cases were reported with full success. The twelfth case was a limited success; the schema translation feature failed, causing an incorrect map icon to appear, however the human operator could still see the icon’s location accurately and compensate mentally. This server error was corrected before the experimentation phase described next.

Additionally, the ability of the BMLC2GUI was enhanced to identify delayed replay cyber intrusion because identifying this by "eyeball" scanning of arriving messages proved impractical.

Table 1: C2SIM Validation Tests in CWIX 2019

Test Number	Test Description	Expected Result
1a	basic connection test: system connects with server; run five times on each client at every node, including back-to-back clients between servers	gets indication of proper connection on each attempt
1b	order submission test: each order source at every node (C2IS or editor) sends order through server to simulation at that node five times	editor at that node and editor at monitor node can see order reflected from server for each order submitted
1c	report submission test: each simulation at every node is placed into a state where it should issue reports; editor at that node editor at monitor node can see five successive reports reflected from the server	editor at monitor node can see five successive reports reflected from the server
1d	basic operation test: individual closed-loop order flow per node - each node individually tests flow from every order source at that node to every simulation at that node for five orders	the resulting reports are observed on order source and on the monitor site editor for five successive reports per order and are verified by human operator to be consistent with the order
2a	system operation test: individual closed-loop order flow among each pair of connected systems - each node individually tests flow from every order source at that node to every simulation in the coalition for five orders	resulting reports are observed on order source and on the monitor site editor for five successive reports per order and are verified by human operator to be consistent with the order
2b	concurrent operation test: parallel closed-loop order flow per node - for a 30 minute period, all nodes concurrently test flow from every order source at that node to every simulation at that node for five orders	resulting reports are observed on all order sources and on the monitor site editor and are verified by human operators to be consistent with the orders sent from their nodes
3a	announced CyberEW emulation test: individual closed-loop order flow per node with CyberEW emulation - for a 30 minute period, each node individually tests flow from every order source at that node to every simulation at that node for five orders, under announced cyber emulation conditions lasting 10 minutes	the resulting reports are observed on order source and on the monitor site editor and are verified by human operator to be consistent with the order and the cyber emulation condition
3b	unannounced CyberEW emulation concurrent operation test: parallel closed- loop order flow per node with CyberEW emulation - for a 60 minute period, all nodes concurrently test flow from every order source at that node to every simulation at that node for five orders under unannounced cyber emulation conditions lasting a total of 10 minutes	resulting reports are observed on all order sources and on the monitor site editor and are monitored by human operators for consistency with the orders; human operators report their observations with regard to at what times a cyber attack was conducted and what options they had to operate successfully while the attack was underway; at least 50% of reports are correct

6. MSG-145 "MiniExercise" Validation

CWIX provided a commendable opportunity to show that six C2 and simulation systems could achieve technical interoperability by implementing the C2SIM draft standard, and also to test the effectiveness of human operators in recognizing cyber effects imposed by the server. However, MSG-145 sought also to verify that the resulting system of systems could support a coalition of international military partners. Therefore, experimentation was conducted in the form of a distributed mission planning exercise, which is one of the MSG-145 focus use cases. The exercise involved supporting a fictional nation called "Bogaland." The national teams participating were augmented by military Subject Matter Experts (SMEs) and conducted a 2-day brigade-level planning exercise. The scenario for this exercise can be summarized as:

- In 2018, NATO ground forces began deploying in Bogaland to assist the Bogaland government in countering the increasingly aggressive activities of a group known as WASA, who are indigenous people of the Norrköping region.
- The WASA are receiving assistance from external nation-states. Information Operations and aggressive military activities have been initiated using the WASA as a surrogate.
- The WASA have been expanding their presence across the region along Highway E4 from Linköping to Norrköping, with the intent to move into Stockholm.
- To support operations, the WASA are using Braviken Bay for logistics operations. Additionally, they are seeking to create a new port at Oxelösund to begin their movement northward to Nyköping.
- As the WASA grows in strength, the Bogaland government requested NATO support to stop WASA's extensive usage of Braviken Bay and counter their movement towards Stockholm along Highway E4 north of Linköping.

The situation involves asymmetric warfare where the Blue force has significant numerical superiority over the Red force, so large encounters are rare; the problem faced by the friendly coalition is to find and suppress the red force. As such, the MiniEx was not conducted with a thinking enemy; the Red forces were largely stationary and only two orders were required to be given to the Red objects. A drawback in the experimentation was that the originally planned Distributed Interactive Simulation (DIS) interconnection turned out shortly before the MiniEx to not be possible, so simulators were not aware of each others' simulated objects. To provide for a reasonable level of Blue/Red interaction, the Red objects which were configured in the same simulations as the Blue force but under orders from the exercise observer station.

Figure 3 compares the one real C2 system (SitaWare) with the BMLC2GUI editor that was used by most participants to enter orders and provide situational awareness. While there can be no doubt that a military operation is likely to be more effective when conducted with SitaWare, the BMLC2GUI proved to be adequate to investigate the military utility of C2SIM. Figures 4, 5 and 6 provide an overview of the Blue and Red sides of the MiniEx scenario as well as the Order of Battle it required to be implemented in the various simulators.

The consensus of all participants in the MiniEx was that C2SIM is functional and not difficult to implement, so it is ready to move forward to balloting as soon as issues detected during the MSG-145 C2SIM validation process are resolved.

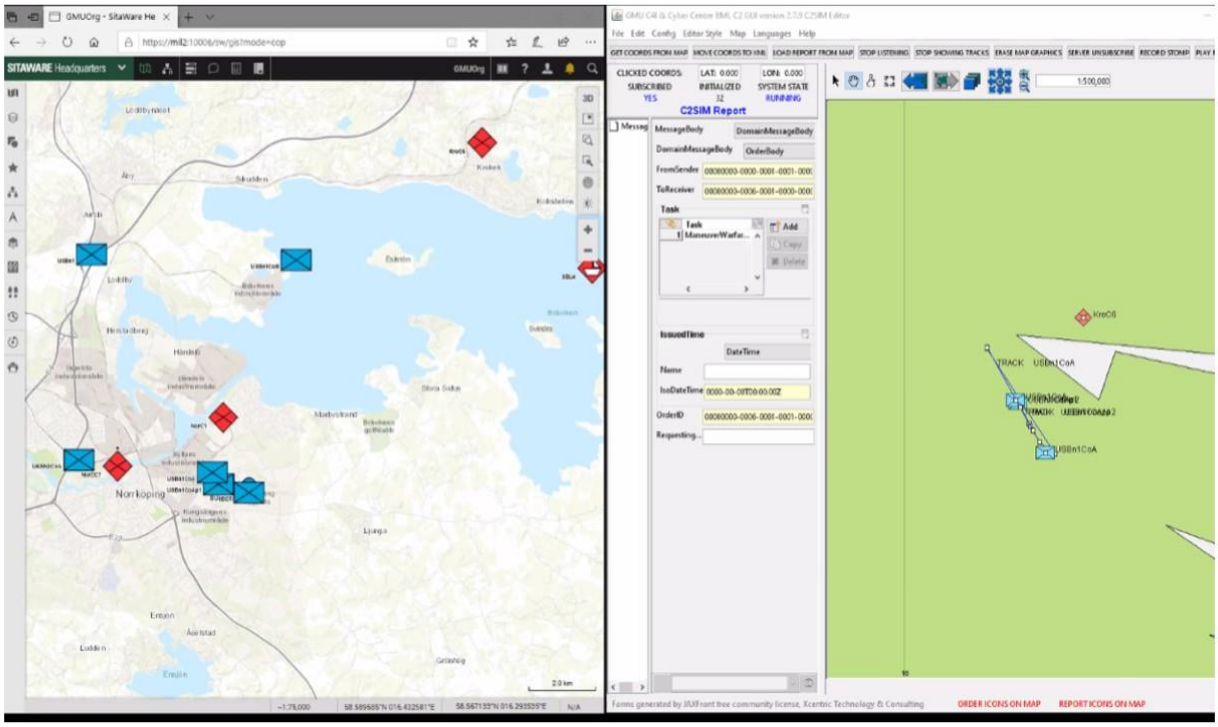

Figure 3: SitaWare and the BMLC2GUI

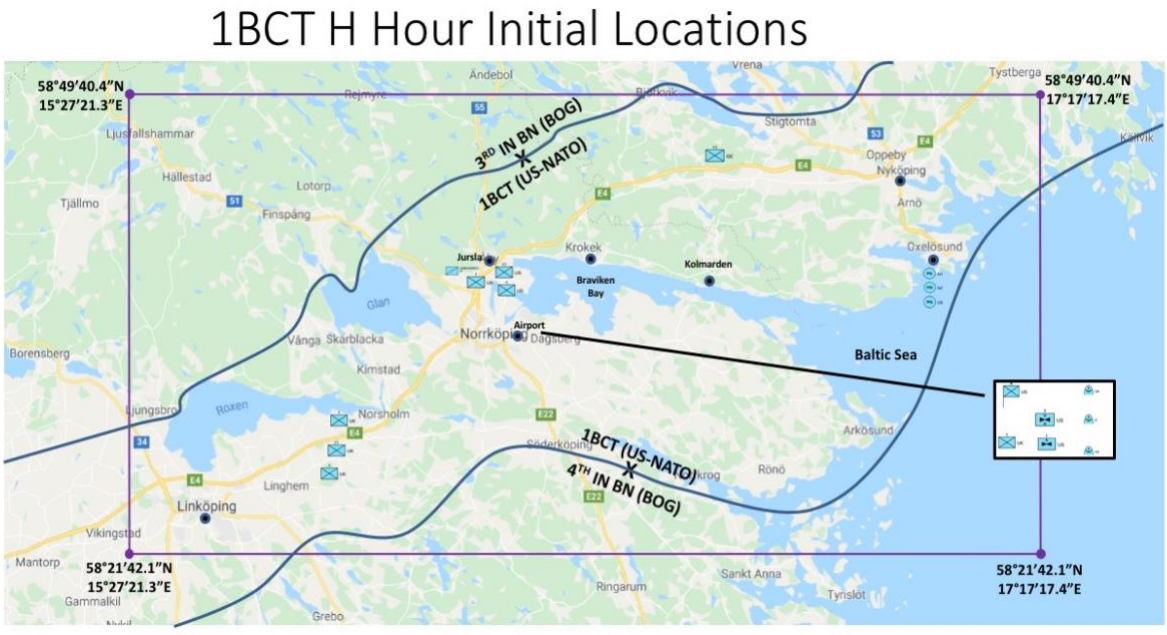

Figure 4: MiniEx Initial Blue Situation

Enemy Situation at H Hour

Figure 5: MiniEx Initial Red Situation

BLUFOR Order of Battle

Unit	Side	Size	Weapons	Sensors	Initial Location at H Hour
1BCT (USA IN)	BLUE	Brigade TF	Small Arms, AH-64, CH-47, UAS, Patrol Boats	FLIR, NVG, UAS Cameras, Binos	FOB vic Norrköping Airport 58.586727N/16.249418E
UAS 1 & 2 (UK)	BLUE	2	None	Camera w/zoom, scan signal	FOB vic Norrköping Airport 58.586727N/16.249418E
UAS 3 & 4 (ITA)	BLUE	2	None	Camera w/zoom, scan signal	FOB vic Norrköping Airport 58.586727N/16.249418E
UAS 5 & 6 (DEU)	BLUE	2	None	Camera w/zoom, scan signal	FOB vic Norrköping Airport 58.586727N/16.249418E
UGV (ITA)	BLUE	1	None	Camera w/zoon, scan signal	FOB vic Norrköping Airport 58.586727N/16.249418E
Maritime Patrol	BLUE	2 Boats (AUS) 1 Boat (NZL) 1 Boat (USA)	TBD	TBD	vic Oxelosund port 58.663903N/17.102725E
D/170th AV RGMT QRF (USA 4 x CH-47, 2 x MH-6)	BLUE	Company	Mix of M4, M5, & M9 MH-6 (gun, rockets, & Hellfire)	NVG, Radio, Binos, Eyes, & NBC	FOB vic Norrköping Airport 58.586727N/16.249418E
C/102nd AV BN (USA AH-64)	BLUE	Company	30mm, Rockets, & Hellfire	IR (thermal), radar, & NVG	FOB vic Norrköping Airport 58.586727N/16.249418E
1/1BCT (USA IN) (Stryker)	BLUE	Battalion	Mix of M4, M5, & M9	NVG, Radio, Binos, Eyes, & NBC	FOB vic Jursla 58.648178N/16.16817E
A/1/1BCT (USA IN)	BLUE	Company	Mix of M4, M5, & M9	NVG, Radio, Binos, Eyes, & NBC	FOB vic Jursla 58.648178N/16.16817E
B/1/1BCT (USA IN)	BLUE	Company	Mix of M4, M5, & M9	NVG, Radio, Binos, Eyes, & NBC	FOB vic Jursla 58.648178N/16.16817E
2ND IN BN (UK)	BLUE	Battalion	Mix of SA80 A2, LSW, & LMG	NVG, Radio, Binos, Eyes, & NBC	vic SW Norrkoping 58.561194N/16.076356E
A/2nd IN BN (UK)	BLUE	Company	Mix of SA80 A2, LSW, & LMG	NVG, Radio, Binos, Eyes, & NBC	vic NW Norrkoping 58.594981N/16.161572E
B/2nd IN BN (UK)	BLUE	Company	Mix of SA80 A2, LSW, & LMG	NVG, Radio, Binos, Eyes, & NBC	vic NW Norrkoping 58.594981N/16.161572E
C/2nd IN BN (UK)	BLUE	Company	Mix of SA80 A2, LSW, & LMG	NVG, Radio, Binos, Eyes, & NBC	FOB vic Norrköping Airport 58.586727N/16.249418E
3RD IN BN (DEU)	BLUE	Battalion	Mix of M4, M5, and M9	NVG, Radio, Binos, Eyes, and NBC	vic Hwy E4 between Norrköping & Nyköping 58.755472N/16.645723E

Figure 6: MiniEx Blue Order of Battle

The MiniEx was conducted in 3 iterations. The first iteration was a communications exercise and walk through (crawl phase) of expected operations. The second iteration provided a walk phase of the tasks practiced in the first iteration and included announced cyber effects. The final iteration was a walk plus phase that included additional orders beyond the second iteration and unannounced cyber effects.

The Brigade Combat Team (BCT) Headquarters (HQ) used SitaWare to display the BCT Common Operational Picture (COP). The US Battalion conducted company operations and attacked a WASA resupply activity. The UK Battalion conducted defensive operations and then non-combatant evacuation operations (NEO) with helicopter units as the WASA escalated their interference in local civil operations. The German Battalion conducted patrolling and attacks on WASA elements. The UK, German, and Italian forces provided Unmanned Aerial Vehicles (UAVs) and establish routes as directed by the BCT HQ. The Italians provided an autonomous Unmanned Ground Vehicle (UGV) that supported US and German movements by conducting route reconnaissance. Additionally, New Zealand provided maritime forces that interdicted supply lines along with US maritime forces. The USA NPS team also conducted attack helicopter operations in iteration 3.

As the MiniEx was executed, each nation's forces executed baseline operations that had been tested during CWIX and then additional tasks were included that increased the complexity of operations. This tested the ability of C2SIM to meet MSG-145's objective of an effective system of systems that could support a coalition of international military partners. This objective was met as a proof of concept with minimal ground unit staffs but would require more resources to extend the period of operations and level of reaction to changes in a BCT combat operation.

Cyber effects were incorporated into the MiniEx as a test of newly developed C2SIM capabilities. The effects worked as planned and the use of announced and then announced effects provided a learning environment for all participants. The potential of including additional cyber or EW effects will be an enhancement to C2SIM. The inclusion of these effects moves C2SIM into an environment that provides a more realistic representation of a cyber-active environment.

Of note is the flexibility of C2SIM to react to changes to the system environment. The UK team was unable to deploy VR Forces as planned and had to revert to JSAF between iteration 1 and 2. Overnight the team reworked its data to be able to participate more effectively in iteration 2 and 3. Also, the New Zealand team incorporated use of VBS3 into the C2SIM system of systems and shared potential expansions of C2SIM integrations from their lessons learned. The lean size of national staffs facilitated some of this flexibility but was also an indicator of the agile ability of C2SIM to react to environmental changes.

7. Conclusions

The validation process reported here gave good confidence that C2SIM is ready for balloting. Problems found during interface development, testing and experimentation were resolved and, where necessary, reported to the C2SIM PDG Drafting Group as indicated needs for changes to the ontology and the XML schema that is derived for it.

Failure to provide DIS interconnection for the simulations in the MiniEx detracted from the realism of the exercise but did not preclude establishing the effectiveness of C2SIM to enable interoperation of coalition C2 and simulation systems.

Therefore, C2SIM appears ready to move ahead to SISO standardization and a NATO STANAG. Upon standard confirmation, the participants in this validation believe it will receive enthusiastic use to enable simulation to support C2 for coalition training, course of action analysis, and mission rehearsal. We expect

to see standardization of the Autonomous Systems Extension and extensions in other domains such as air and maritime operations and also maturation of the ontologies under control of the SISO C2SIM PSG as usage indicates need for additional data classes and properties.

References

[1] Sudnikovich, W., J. Pullen, M. Kleiner, and S. Carey, "Extensible Battle Management Language as a Transformation Enabler," in SIMULATION, 80:669-680, 2004

[2] Pullen, J., B. Patel, and L. Khimeche, "C2-Simulation Interoperability for Operational Hybrid Environments," NATO Modelling and Simulation Symposium 2016, Bucharest, Romania.

[3] Simulation Interoperability Standards Organization, *Standard for: Military Scenario Definition Language (MSDL)*, 2009

[4] Simulation Interoperability Standards Organization, *Standard for: Coalition Battle Management Language (C-BML)*, 2012

[5] NATO Collaboration Support office, *MSG-085 Standardization for Command and Control – Simulation interoperability: Final Report*, July 2015

[6] Simulation Interoperability Standards Organization, *Product Nomination for Command and Control Systems – Simulation Systems Interoperation*, July 2014

[7] Pullen, J. "A Distributed Development Environment for a C2SIM System of Systems," *International Command and Control Research and Technology Symposium 2017*, Los Angeles, CA, November 2017

[8] Pullen, J. and J. Ruth, "Training Operational Military Organizations in a Cyber-active Environment Using C2-Simulation Interoperation," *International Command and Control Technology Symposium 2018*, Pensacola, Florida, November 2018

[9] Allied Command Transformation (ACT) CWIX, https://www.act.nato.int/cwix, viewed 12 July 2019

[10] Pullen, J., D. Corner, R. Wittman, A. Brook, P. Gustavsson, U. Schade and T. Remmersmann, "Multi-Schema and Multi-Server advances for C2-Simulation Interoperation in MSG-085," NATO Modelling and Simulation Symposium 2013, Sydney, Australia, October 2013