C2SIM in CWIX:
Distributed Development and Testing for Multinational Interoperability

Dr. J. Mark Pullen
Center of Excellence in C4I and Cyber
George Mason University
4400 University Drive
Fairfax, VA 22030
USA

mpullen@c4i.gmu.edu

Lionel Khimeche
Direction générale de l'armement
16 bis, avenue Prieur de la Côte d'Or
94114 Arcueil cedex
FRANCE

lionel.khimeche@intradef.gouv.fr

Kevin Galvin
Thales Research & Technology
350 Longwater Avenue, Green Park,
Reading, RG2 6GF
UNITED KINGDOM

Kevin.Galvin@uk.thalesgroup.com

ABSTRACT

Technical Activities in the NMSG have conducted a sustained effort to develop a standards-based capability for coalitions to interoperate their national command and control (C2) and simulation systems collectively. This form of multinational interoperability can have a great impact on the effectiveness of coalition military operations. The technical basis for C2SIM is the second generation of SISO standards for C2-simulation interoperation. This is being built by converging first generation capabilities (MSDL and C-BML) in a way that is designed to be extensible to many domains. The second generation must be tested before it is standardized; the experience gained also will be needed for a STANAG.

C2SIM must have compelling tests to provide confidence. MSG-145 has stimulated development of a 24x7 demonstration and testing capability called the C2SIM Sandbox and is using it to conduct demonstrations at multiple events where C2SIM is exposed to military operators, culminating in CWIX. This paper describes testing achieved at CWIX 2018, including the role of the C2SIM Sandbox in its development, and also plans for distributed experimentation and advanced testing in CWIX 2019, including effectiveness of server-imposed cyber effects. Preparing for SISO standardization as a basis for a STANAG requires showing value to the operational military community. Hence, it is expected to perform additional tests within a broader scope including Federated Mission Networking (FMN) in order for M&S to be fully addressed in its spiral 4 specifications.

1.0 INTRODUCTION

Over the past ten years, a new approach has been developed to integrate coalition command and control (C2) systems and simulations into a complex system of systems. Teams from twelve NATO nations have worked together toward a vision that a coalition will be able to assemble such a complex system rapidly in a standards-based environment called Command and Control – Simulation Interoperation (C2SIM), with the result that each nation uses the national C2 system with which it has trained and that its forces are represented by a national simulation built around its capabilities and doctrine [1]. The resulting technology is being developed under auspices of the NATO Modelling and Simulation Group (NMSG) and standardized by the Simulation Interoperability Standards Organization (SISO) [2]. This emerging capability is now advancing toward military operationalization. More details can be found in [3] and [4].

Military command and control (C2) in a coalition environment, where each nation is likely to have different doctrine, equipment, and C2 information system (C2IS, also called C2 system), presents many challenges. The difficulty is even greater where the national forces in the coalition are capable of incorporating simulations to increase the functionality of their C2IS. This paper reports on progress in developing standardized methods for military coalitions to interoperate C2 systems and simulations as a system-of-systems, resulting in improved functionality, timeliness, and cost savings [5]. Simulations are useful as C2 system elements for course of action (COA) analysis and to stimulate training and mission rehearsal (including wargaming) [6].

Coalitions consist of military forces from multiple nations; generally, each national force has its own C2 and simulation systems, which complicates the problem of operating as a cohesive whole. The goal of C2SIM is to enable an environment where national C2 systems can exchange information freely and each nation's military operations can be represented accurately, with each nation's force representing their own military operations by means of their own simulations. In developing C2SIM technology and standards, we look forward to a day when a newly-formed coalition, operating over a shared network, can "plug in" their C2 and simulation systems to the network and work together rapidly and seamlessly to train, analyze COAs, and perform mission rehearsal. As a result, the coalition will able to perform these functions as a cohesive whole and do so more rapidly and efficiently.

Within such a force, the C2 systems may function as a group using a C2 interoperation capability such as the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) [7] and the simulations may function as a group using an interoperation capability such as Distributed Interactive Simulation (DIS) [8] or High Level Architecture (HLA) [9]. Alternately, it is possible for all systems to share information through the C2SIM capability, although the resulting system may have less detailed time resolution. We refer to the totality of systems interoperating under C2SIM as a *coalition*, just as a collection of simulations interoperating under the HLA is called a *federation*.

The remainder of this paper is organized as follows: Section 2 describes the Simulation Interoperability Standards Organization (SISO) activities that are essential for C2SIM; Section 3 provides an overview of the NATO role in producing and validating the current C2SIM technology. Section 4 describes the distributed development environment known as *C2SIM Sandbox* that is used by NATO MSG-145 to deploy and test C2SIM; Section 5 describes how this capability can be used for operational training under cyber-active conditions; section 6 describes C2SIM testing in NATO Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) 2017 and 2018. Section 7 describes MSG-145 plans for continued and expanded testing of C2SIM in an operational environment and Section 8 concludes the paper.

2.0 SISO C2SIM ACTIVITIES

SISO's mission is to develop, manage, maintain, and promulgate user-driven Modelling and Simulation (M&S) standards that improve the technical quality and cost efficiency of M&S implementations across the world-wide M&S community. SISO seeks to foster the open exchange of information and technologies to support the advancement and standardization of M&S-related technologies and practices. Its work is done by companies or other organizations and by individuals volunteering their efforts.

2.1 First Generation Standards: MSDL and C-BML

SISO's development of C2SIM standards began with two loosely coupled, parallel efforts to standardize the C2 to simulation technologies. These were the Military Scenario Development Language (MSDL) [10] and the Coalition Battle Management Language (C-BML) [11]. MSDL provides for consistent initialization/start-up data for both C2 and Simulation systems participating within a coalition. The object standardized by MSDL is the *scenario file*, which provides a specific description of the situation and course of action at a moment in time for each element in the scenario. C-BML grew out of a US Army experiment that sought ways to replace the natural language of battlefield C2 with an unambiguous language that can be used as input to software [6]. The C-BML standard defines standard XML data composites for tasking (orders and requests) and reports.

NATO M&S Technical Activities described below have helped to shape C2SIM. For example, experimentation in MSG-048 determined that, for an effective operational capability, the SISO C-BML focus on Orders, Requests and Reports needs to be supplemented with initialization via MSDL in order to address the full scope of C2SIM.

2.2 Second Generation Standard: C2SIM

NATO MSG-085 successfully demonstrated technical and operational relevance, and in so doing built considerable experience that helped in completing the C-BML Phase 1 standard. However, MSG-085 also produced clear results [12] indicating a need for more work by SISO. MSDL and C-BML were developed separately and are less than perfectly suited to working together; an integrated standard is needed. Also, C-BML Phase 1 requires extension in order to be used for the full spectrum of military operations.

MSDL and C-BML each had been intended to move forward to at least one more version. The Product Development Groups responsible for the two standards saw significant benefit in combining their efforts in the second phase of each. They therefore proposed a new, unified effort to replace the second phase of MSDL and C-BML: a single C2SIM Product Development Group for C2-simulation interoperation, to include other systems dependent on the same information (e.g. autonomous or robotic systems), which is planned to consist of four documents: (1) The C2SIM Standard, consisting of overall standard structure with procedures and message flow for initialization and tasking/reporting; (2) The C2SIM Core Ontology, which contains a set of data classes defining logical data model (LDM) that are expected to be needed by all, or nearly all, domains that implement C2SIM; (3) a Guideline document for implementing C2SIM, and (4) an example Maneuver Warfare extension to the Core, providing for interoperability similar to that embodied in MSDL and C-BML.

After the SISO C2SIM Standard is adopted, a variety of additional extensions are likely to be considered. For example, there is ongoing interest in expanding C2SIM to autonomous systems [13].

3.0 NATO C2SIM ACTIVITIES

SISO has neither technology development capability nor military forces that can evaluate technologies; for C2SIM these roles are performed by national teams from NATO.

The need for C2SIM interoperation is particularly acute in coalitions. Differences among coalition partners' C2 systems make use of a single system impractical, while differences in organization, equipment, and doctrine result in a situation where each national simulation system may represent only the sponsoring nation's forces well. Since 2005 groups from the NMSG have been working toward this shared vision [2]:

> *The year is 2025, and somewhere in the vicinity of the North Atlantic a need has arisen for a military force to perform a peacekeeping mission. NATO has agreed to deploy a Multinational Brigade for this mission, and three of its member nations have agreed to provide forces. The designated military organizations promptly connect their command and control (C2) and simulation systems over a secure network and begin training together for their new, common mission. Each nation's forces are commanded by their own C2 system, which they understand well from long experience; also each nation's forces are represented in virtual engagements by their own simulation, which reflects accurately their personnel, equipment, and doctrine. As a result, the coalition force is able to prepare rapidly for its new mission, learning to deal with the unique aspects of each national force while preparing those forces to work together toward their shared mission.*

The NMSG has organized a sequence of Technical Activities to work toward this vision. C2-simulation interoperation technology originally was called "Battle Management Language" (BML). The general architecture adopted for that work, based on Web Services, is shown in Figure 1. It has continued to be used for succeeding NMSG work in C2SIM. MSG-048 Coalition Battle Management Language and MSG-085 Standardization for C2-Simulation Interoperation demonstrated first technical feasibility, then military utility of C2SIM. Currently MSG-145 is aimed at Operationalization of Standardized C2-Simulation Interoperability.

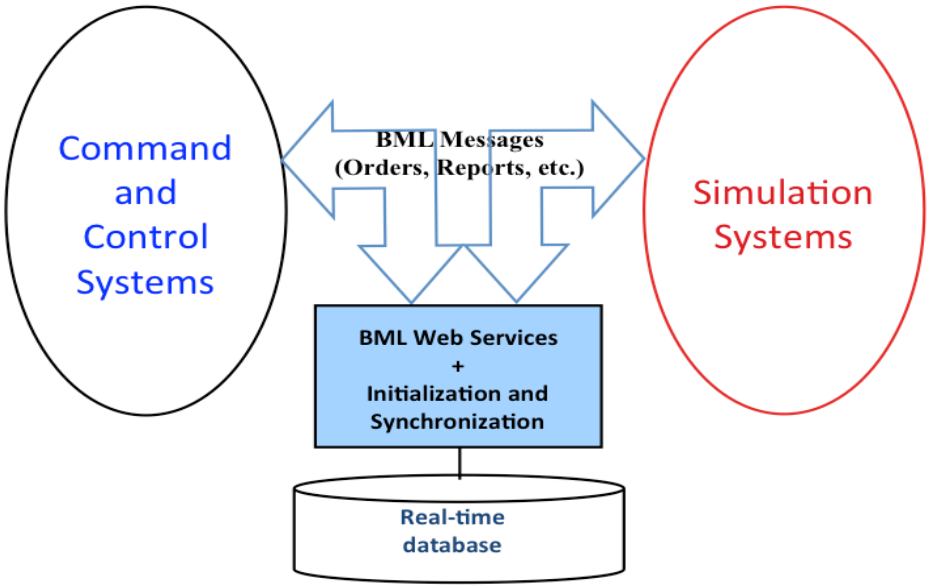

Figure 1: General Architecture for C2SIM

Collectively, these activities have developed, demonstrated, and validated the required technology for C2SIM. At various times Belgium, Canada, Denmark, France, Germany, Netherlands, Norway, Spain, Sweden, Turkey, the United Kingdom (UK) and the United States of America (USA) have participated. In doing so they have effectively complemented the standardization work of SISO. Ultimately, MSG-145 intends to put forward the SISO C2SIM standard as a NATO Standardization Agreement (STANAG).

The Final Demonstration of MSG-085 took place at Fort Leavenworth, Kansas in December, 2013. MSG-085 partnered with the US Army Mission Command Battle Laboratory, first engaging in a short integration session. The featured capability was Joint and Combined Mission Planning. The architecture of the demonstration system-of-systems that was assembled is shown in Figure 2. In addition to establishing the operational relevance of the approach, this demonstration showed that the technology used had achieved a greatly improved technology readiness level (TRL). This was shown by expeditious integration of the various systems used and also by a capability for operation over the Internet. The MSG-085 final audience got the message "We have an exciting new capability and it works very well to improve some unmet needs of coalition C2, using interoperable simulations." MSG-085 finished its work in 2014 [14, 15].

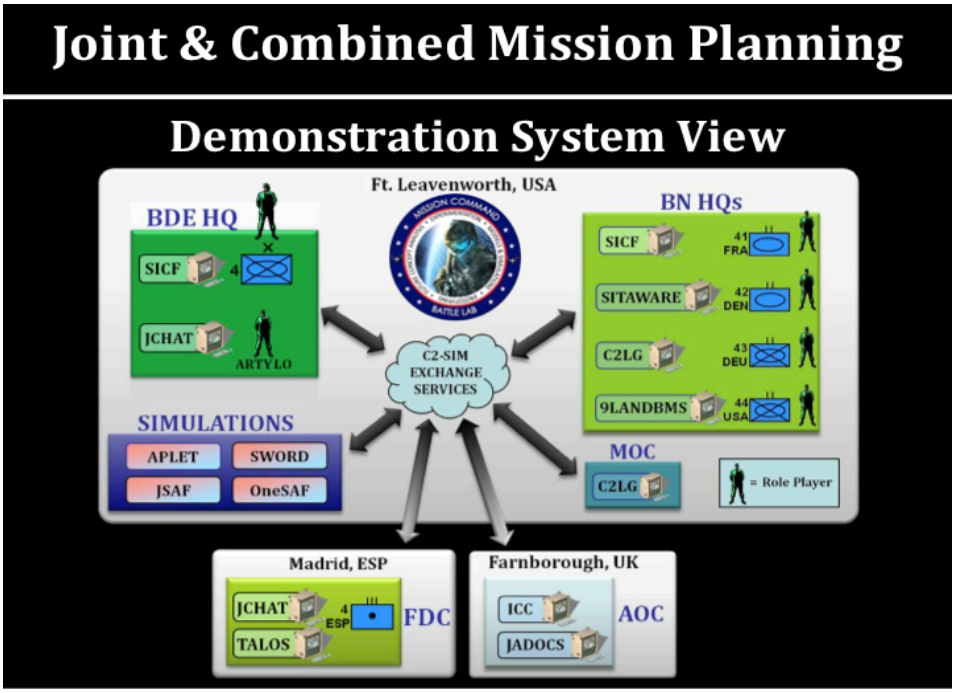

Figure 2: MSG-085 Final Demonstration System of Systems

4.0 DISTRIBUTED DEVELOPMENT IN NATO C2SIM

From their inception, NMSG activities in C2SIM have been faced with the problem of integrating and testing software developed by several national teams into a coherent system of systems that can support experimentation and demonstrations. While adopting Web Service architecture and a well-coordinated sequence of schemata facilitated this, problems of technical and cultural adaptation among multiple national teams remained, due to the fact the software systems and their developers had not previously worked together. Initial response to these problems was to periodically co-locate the teams for integration and testing. This was an expensive approach because of travel involved and it necessarily constrained the time available for integration and testing to a tight schedule. For MSG-048, this caused difficulties in that a planned week of

final integration at Portsmouth, UK, proved insufficient so that an extra week in Paris, France had to be scheduled on short notice. Even after this extra time, the MSG-048 Final Experimentation began with some systems not interoperating; in fact the whole system-of-systems became fully functional only on the last day of experimentation. (Those operational military who participated in the experimentation nevertheless saw great potential in C2SIM and encouraged its continued development.)

4.1 Internet-Based Distributed Development

In order to facilitate continued integration during MSG-085, a Virtual Private Network (VPN) was established over the Internet, available to all participating national teams, providing continuous access to instances of both of the C-BML/MSDL servers used in MSG-085. National teams who needed to test C2 and simulation systems could schedule use of this facility, typically by two or three teams testing together. In this way, many integration problems could be resolved without travel. Combined with the evolving maturity of MSDL and C-BML implementations, this resulted in a much more coherent process when MSG-085 teams came together for a final week of testing at Copenhagen in October 2013 before the final demonstration. While some problems remained, the participating teams left that week with a solidly functional C2SIM system-of-systems. On reassembling at Fort Leavenworth, Kansas in December, 2013 there were a few minimal problems due to last minute changes but the observation was that the system of systems "plugged together and worked."

4.2 C2SIM Sandbox

Integration and testing has been a significant challenge in developing C2SIM. Initially, an XML schema developed by one team was exchanged among the participating national teams. As described above, this formed the basis for quarterly integration and testing sessions where all teams assembled at a common location. Given the style differences among national teams involved, the integration process was both technical and social in nature and clearly was necessary in order to arrive at an integrated whole. However, it proved very expensive in terms of developer travel and the cost seemed likely to increase as the schemata evolved to become more complex during the standardization process. As described above, MSG-085 arrived at a style of Internet-based development and testing, consistent with the fact that the intended product was designed for distributed operation in a networked environment. The new style started as a VPN enclave, where any of the national teams could work with the same server to test and/or demonstrate C2SIM functionality. In MSG-145, that environment has expanded to become a full C2SIM capability, available over the VPN by remote desktop technology, allowing national teams to test and demonstrate any combination of C2 systems, simulation systems, and servers in the "C2SIM Sandbox." The capability includes the open source Internet-based audio/video/whiteboard/chat conferencing system Jitsi [16], which greatly facilitates group communication.

The C2SIM Sandbox provides a continually available environment, available by VPN to national teams to test and demonstrate C2SIM. It supports the initial trial SISO C2SIM core developed for CWIX, including capabilities for orders, reports, and initializations. In addition to these functions, the C2SIM Sandbox is building experience toward a future "C2SIM as a Service" capability [17]. This has begun by using the C2SIM Sandbox as the nucleus of a distributed testbed operated for MSG-145. Development and testing for CWIX 2018 deployment took good advantage of these capabilities.

The C2SIM Sandbox currently employs the BMLC2GUI system [18] as a surrogate for C2, the VT-MÄK commercial combat simulation VRForces [19], and an open source server, operating in a virtual computing environment. The server is the C2SIM Reference Implementation server developed for the SISO C2SIM standards effort (see section 4.3 below); it features interoperation with MSDL, C-BML and IBML09 through schema translation. The Sandbox has been tested with external C2IS NORCCIS/SWAP and simulations JSAF and KORA in CWIX (see section 5 below).

An important capability employed in the Sandbox is virtual/remote desktop via Web browser, which recently has become available commercially in Apache Guacamole [21]. This enables remote participants to work with any application incorporated in the Sandbox, using only readily available open source VPN client and any HTML5 compliant web browser. The Sandbox environment uses open source remote desktop gateway software and virtual network computing (VNC) to enable remote interaction with virtual machines hosted within a VMWare vSphere hypervisor as well as actual physical machines. The virtualized environment allows for flexibility in the applications and services made available for testing.

C2SIM Sandbox remote application interfaces are intentionally limited to the user GUI capability of each software system. The Sandbox is able to block inspection of the C2, simulation or server code so that privacy can be provided for software providers. For Windows systems, this is accomplished using a combination of group policy controls to operate the system in a kiosk mode. Instead of physical interaction, users work remotely through the remote desktop gateway accessed within the Sandbox environment's virtual private network. A similar capability is achieved on Linux systems using a window manager optimized for restricting application access.

A pre-packaged scenario from CWIX 2018 with recorded instructions for operation is included with the Sandbox, to enable the C2SIM configuration to be exercised with only a minimal understanding of the software. The scenario is user-modifiable within a limited scope via the C2 system GUI, to allow users to run alternatives and observe results.

4.3 C2SIM Reference Implementation Server

The C2SIM Sandbox server is a new open-source Java-based server, developed by the GMU C4I and Cyber Center as a reference implementation for the C2SIM LDM Core and Maneuver Warfare extension. It is a further development based the WISE-SBML translating server approach described in [20], which is capable of translating among XML documents based on different schemata if they are semantically-equivalent, which also will be easier to reconfigure. This provides a means of backward compatibility from C2SIM to first-generation BML standards MSDL and C-BML. Use of Java is intended to make the server more portable and understandable, at the cost of lower performance than WISE-SBML; it nevertheless has shown transaction rates in excess of 200 reports per second. Like its predecessors, the server supports logging and replay; it also includes support for late joiners and checkpoint/restart.

Figure 3 shows the architecture of the C2SIM Sandbox, including the C2, simulation, server, scheduling, and collaboration/conferencing components. All of these are intended to be accessed remotely, via a Web browser. In addition to interacting with the sandbox components (individually or at multiple remote VPN sites), the systems in the Sandbox are able to interact over the VPN via C2SIM standards with other C2 systems, simulation systems, or server systems.

Thus the C2SIM Sandbox is able to facilitate testing and demonstration in a variety of modes:

- C2SIM demonstrations
  - Schemata: IBML09, CBML Light, C2SIM Core
  - C2SIM Maneuver Warfare when available
  - Generic scenario provided (others if contributed)
- C2SIM testing
  - Test C2 with Sandbox Server and Simulation
  - Test Server with Sandbox C2 and Simulation
  - Test Simulation with Sandbox C2 and Server
  - Test C2-Simulation Coalitions with the Server

- Distributed configurations of all sorts
- C2SIM validation with SISO
- C2SIM-based exercises (scope limited by server performance)
- In the future: C2SIM as a Service. To prepare for this, MSG-145 through TNO, Netherlands are developing a C2SIM Reference Architecture. This architecture builds on the NATO C3 Taxonomy and Modeling and Simulation as a Service (MSaaS) Reference Architecture.

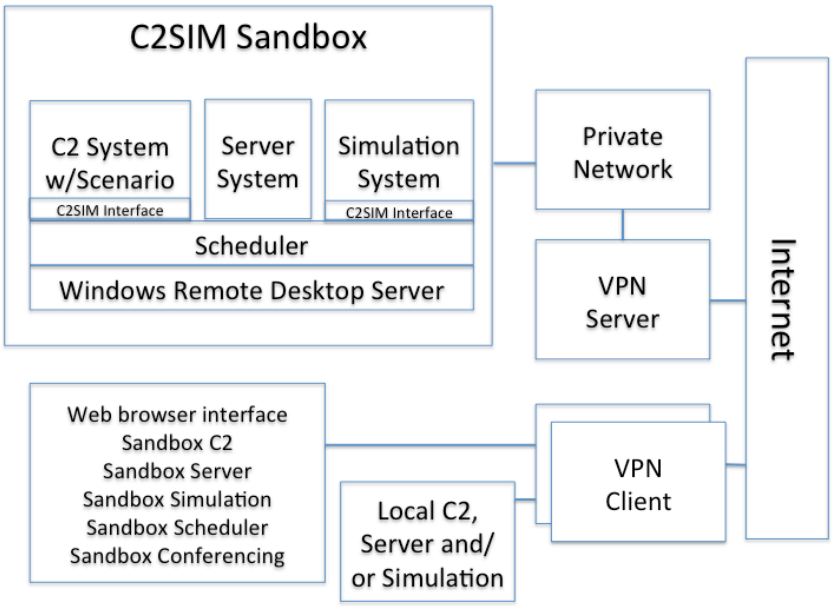

Figure 3. C2SIM Sandbox Architecture

5.0 C2SIM SANDBOX CYBER TRAINING CAPABILITY

Cybersecurity has become a major concern in military operations. This implies a need for operational training. There are two general areas of training for cyber security: (1) training specialized to cyber operations and (2) regular military operational training that applies to a cyber-active environment. A new C2SIM Sandbox capability applies to the latter, which is quite important because military forces must be prepared to function effectively in the cyber-active environment [22].

Establishing a cyber-active training environment for operational military units is difficult because: (1) a live training environment that allows real cyber-attacks on the information systems supporting an exercise would be so disruptive as to immediately halt any other training; and (2) real time modification of C2 information systems to emulate an attack would be expensive and detrimental to readiness, especially so in coalitions where every system would have to be modified and subsequently reimaged. The C2SIM Sandbox Cyber capability introduces cyber-attacks at the C2SIM server and focuses on mitigating the introduced cyber effect without damage to unit C2 assets and allows the cyber effects to be introduced in a controlled manner.

First practical trial uses of C2SIM for training in a cyber-active environment occurred in NATO CWIX 2017 and 2018, using the Reference Implementation C2SIM server, with the intention of evaluating how C2SIM could support this established military need:

> *"The Department of Defense information network-Army (DODIN-A) is an essential warfighting platform foundational to the success of all unified land operations. Effectively operating, securing, and defending this network and associated data is essential to the success of commanders at all echelons. We must anticipate that future enemies and adversaries will persistently attempt to infiltrate, exploit, and degrade access to our networks and data. In the future, as adversary and enemy capabilities grow, our ability to dominate cyberspace and the [electromagnetic spectrum] EMS will become more complex and critical to mission success. ... Incorporating cyberspace electromagnetic activities (CEMA) throughout all phases of an operation is key to obtaining and maintaining freedom of maneuver in cyberspace and the electromagnetic spectrum (EMS) while denying the same to enemies and adversaries." Forward, FM 3-12, April 2017 [23]*

As training progresses, cyber concepts and effects must be introduced in order to prepare military personnel. Ultimately, training must allow participants to confront a determined foe that is attempting to gain control of the cyber environment and affect coalition activities. Leaders must understand and accept the risks associated with degraded/denied cyber environmental conditions in exercises and foster an ability to overcome negative performance impacts as a result of conducting operations in a contested training environment [24].

It is possible to apply many of the effects of cyber and electronic warfare attacks by modifying the C2 messages as they flow through the C2SIM server, as shown in Figure 4. The significant difference between Figure 1 and Figure 4 is the addition of a cyber effects editor and an exercise driver that work together to impose CEMA effects on the C2 message stream, creating the effect of a cyber-active environment. While this idea is not new, its impact is greatly expanded when employed in a standards-based coalition environment. Some experience with a similar approach has been obtained with the US Navy's NE2S system [25] and the US Army's OneSAF prototype Cyber Operations Battlefield Web Service (COBWebS) [26]. In each of these systems, all effects have been imposed in a single simulation.

As shown in Figure 4, the modified C2SIM server emulates cyber effects by modifying or deleting messages passing through C2SIM servers. It operates under control of a script which can be invoked by events in the exercise or during specific periods of time and can modify or delete the C2 messages selectively for specific systems or even specific simulated force elements. The server has been evaluated on a limited testing basis in CWIX 2017 and 2018. In 2017, only EW effects (jamming) were introduced. In 2018 the full list of effects described below were available; the testing included EW jamming and cyber-effects of modifying messaging.

Using the Cyber Effects Editor, cyber attacks may be initiated, modified, and terminated under operator control during server operation. Controls for the editor take the form of XML messages in the web service input stream. A separate log file captures for later analysis all cyber-related activity including command submission and attacks conducted. Cyber script commands are submitted by the controller of the cyber environment. Each submission of a new cyber command language file cancels any attacks in operation at that time and can start new attacks or stop all attacks. Details are available in [27].

6.0 TESTING C2SIM IN CWIX 2018

Testing was accomplished using the Norwegian C2 system NORCCIS/SWAP, the German training simulation KORA, the JSAF simulation run by the United Kingdom, and the commercial military simulation VR-Forces from VT-MAK as interfaced in the C2SIM Sandbox. Out of seventeen tests, fourteen were completely successful, three could not be held due to network problems, and two were classed as "limited success" due to

software issues that were resolved and corrected before the end of the testing period. Three of the twelve hours of testing were configured as variations on previous successful tests with the addition of CEMA effects; these were among the fully successful tests from a technology standpoint.

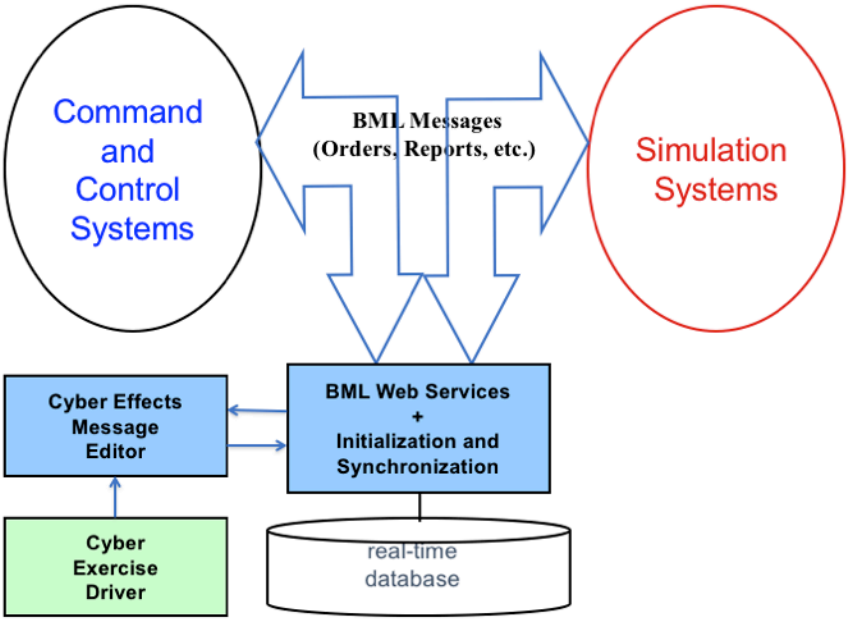

Figure 4: C2SIM architecture with cyber effects Imposed on C2 messages

6.1 Cyber Testing in CWIX 2018

In the initial Cyber evaluation during CWIX 2018, C2SIM CEMA effects were tested as part of the first major tests of C2SIM. CWIX 2018 was an initial technology test for cyber effects imposed in the server. C2SIM Cyber Effects Message Editor was implemented in an environment with limited users and a limited observation plan. As cyber threats are introduced, observers measured the impact of the threat on operations and captured the elapsed time available for users to take countermeasures. However, due to the limited size of the C2SIM contingent at CWIX limited time available to develop testing procedures, the results are simply a statement that everything worked for the two effects tested. MSG-145 is planning a much larger set of tests for 2019, both before and during CWIX, that will include human role-players. We expect this will provide a much more thorough evaluation of the effect of imposing CEMA effects in a C2SIM server.

7.0 MSG-145 PLANS FOR EXPANDED TESTING OF C2SIM

MSG-145 is preparing to perform a thorough and highly credible evaluation of the forthcoming SISO C2SIM standard, through experimentation and testing. A sequence of activities has been planned, starting in September 2018 and culminating with significant experimentation followed by expanded CWIX 2019 testing. The experiments are planned to be similar in scope to the demonstration at Fort Leavenworth in 2013 that established the military utility of the CSIM approach, but fully distributed among the participating nations in order to add credibility and reduce expense. The schedule is:

- September 2018: national teams commit to participate
- October 2018: specific national role-players identified

- November 2018: trial use by CWIX 2018 participants of C2SIM schema derived from balloted SISO C2SIM standard (Core + Maneuver Warfare)
- December 2018: demonstrate first use of schema based on C2SIM standard
- January 2019: all other nations test using standardized schema
- February 2019: system-of-systems test using standardized schema
- March 2019: distributed experimentation using system-of-systems with role players
- May 2019: distributed mini-exercise with role players, including cyber effects
- June 2019: subgroup reproduces a slice of mini-exercise in CWIX 2019, working with Federated Mission Network and M&S as a Service

The cyber aspect of this plan is particularly important. Without competent active or retired military SME role players, it would not be possible to evaluate the pros and cons of the approach described above to training with server-imposed cyber effects.

8.0 CONCLUSIONS

Working together, SISO and NATO MSG have developed a powerful new approach to interoperating command and control with simulation in coalition operations and training. The approach has been enabled by VPN-based distributed development involving multiple national teams and facilitated by a unified remotely-accessible C2SIM platform called C2SIM Sandbox.

Using C2SIM Sandbox, CWIX 2018 provided a successful initial test for C2SIM with one C2 system and three simulations, including a limited set of cyber behaviors using the approach described in this paper. A much more thorough test of the C2SIM standard as it goes to SISO balloting is planned for 2019. This will include distributed human role-players and additional cyber behaviors. Testing will validate C2SIM (Core and Maneuver Warfare Extension) as put forward for standardization and will include evaluation of cyber effects by the SME role players.

C2SIM holds significant promise as a force multiplier technology for NATO. Efforts of the NATO MSG have illuminated this promise and moved the capability toward operational use. Latest activity includes preparing for more CWIX testing as part of distributed operational evaluation in 2019.

REFERENCES

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

[2] Pullen, J. *et al.*, “Developing Effective Standards for C2-Simulation Interoperability,” NATO Modelling and Simulation Symposium 2015, Munich, Germany, October 2015

[3] Pullen J. and K. Galvin, “New Directions for C2-Simulation Interoperability Standards,” International Command and Control Research and Technology Symposium 2016, London, UK

[4] 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

[5] Pullen, J. and O. Mevassvik, “Coalition Command and Control – Simulation Interoperation as a System of Systems,” IEEE 11th International Conference on System of Systems Engineering (SoSE 2016) June 12th – 16th, 2016 Kongsberg, Norway

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

[7] Multilateral Interoperability Programme, 2007, *The Joint C3 Information Exchange Data Model (JC3IEDM) Edition 3.1a*.

[8] IEEE Standards Association, 2010, *IEEE Standard 1516, High Level Architecture for Modeling and Simulation*.

[9] IEEE Standards Association, 2012, *IEEE Standard 1278.1, Distributed Interactive Simulation*.

[10] Simulation Interoperability Standards Organization, *Standard for: Military Scenario Definition Language (MSDL),* 2008.

[11] Simulation Interoperability Standards Organization, *Standard for: Coalition Battle Management Language (C-BML),* 2014

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

[13] Biagini, M., F. Corona, M. Wolski and U. Schade, "Conceptual Scenario Supporting Extension of C2SIM to Autonomous Systems," International Command And Control Research and Technology Symposium 2017, Los Angeles, CA, 2017

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

[15] Gautreau, B., L. Khimeche, J. Martinet, E. Pedersen, J. Lillesoe, D. Liberg, T. Remmersmann, D. Muniz, T. Serrano, N. Dereus, H. Henderson, "Lessons Learned from NMSG-085 CIG Land Operation Demonstration," IEEE Spring Simulation Interoperability Workshop, San Diego, CA, 2013

[16] Jitsi, *Wikipedia* https://en.wikipedia.org/wiki/Jitsi, viewed 31 July 2018

[17] NATO Collaboration Support Office, "MSG-136 Modelling and Simulation as a Service," https://www.cso.nato.int/ACTIVITY_META.asp?ACT=5642, viewed 31 July 2018

[18] Ababneh, M. and J. Pullen, "An Open Source Graphical User Interface Surrogate C2 System for Battle Management Language Experimentation," 16th International Command and Control Research and Technology Symposium, Quebec, Canada, June 2011

[19] VT-MAK VR-Forces, https://www.mak.com/products/simulate/vr-forces, viewed 31 July 2018

[20] 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

[21] Apache Guacamole https://guacamole.apache.org, viewed 31 July 2018

[22] Pullen, J. and J. Ruth, "Training Operational Military Organizations in a Cyber-active Environment Using C2-Simulation Interoperation," International Command and Control Research and Technology Symposium 2017, Pensacola, FL, November 2018

[23] U.S. Army Field Manual 3-12, Cyberspace and Electronic Warfare Operations, April 2017.

[24] Wells, D., and D. Bryan, Cyber Operational Architecture Training System – Cyber for All, Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2015 Paper Number 15108.

[25] Naval Air Warfare Center, Network Effects Emulation System (NE2S)/Cyber Operational Architecture Training System (COATS), http://www.navair.navy.mil/nawctsd/pdf/5-2014 COATS NE2S.pdf downloaded 22 May 2018.

[26] U.S. Army Research Laboratory, Open Campus, Cyber Battlefield Operating System Simulation Tools for Live-Virtual-Constructive (LVC) Training Simulations, https://www.arl.army.mil/opencampus/sites/default/files/HS05.pdf, downloaded 25 May 2018

[27] Pullen, J. and J. Ruth, "Military Training Operational Military in a Cyber-active Environment Exploiting C2-Simulation Interoperation," SISO Workshop, Orlando, FL, September 2018