**23rd ICCRTS**
**"Multi-Domain C2"**

**Title**

Training Operational Military Organizations in a Cyber-active Environment Using C2-Simulation Interoperation

**Topics**

Interoperability, Integration and Security

**Names of Authors**

J. Mark Pullen
George Mason University

James Ruth
Trideum Corporation

**Point of Contact**

J. Mark Pullen
George Mason University C4I and Cyber Center
Fairfax, VA 22030
703-993-3682
mpullen@c4i.gmu.edu

# Training Operational Military Organizations in a Cyber-active Environment Using C2-Simulation Interoperation

J. Mark Pullen
G4I & Cyber Center
George Mason University
4400 University Drive
Fairfax, VA 22030
mpullen@c4i.gmu.edu

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

Keywords: military training, cyber-active, command and control-simulation interoperation

**Abstract**

Critical needs in a cyber-active environment include both training cybersecurity technical personnel to provide for defense of operational systems and preparing operational military organizations to continue to function in such an environment. The latter is mostly unmet today, for two reasons: (1) a real cyber-attack on the information systems supporting an exercise would be so disruptive as to preclude any other training; and (2) modifying those supporting information systems to emulate an attack would be expensive, especially so in coalitions where every system would have to be modified.

The authors have reported in previous ICCRTS on the Command and Control - Simulation Interoperation (C2SIM) capability which enables a coalition to interoperate their C2 and simulation systems for training, course of action evaluation, and mission rehearsal. Typically, C2SIM information is exchanged via interface to a server. Reviewing capabilities introduced for single systems such as the Network Effects Emulation System (NE2S) simulation, we recognized the C2SIM server as an ideal place to emulate a wide range of cyberattack effects by modifying or deleting information as would happen from compromised software or networks and electronic warfare attacks. This requires the operational military organization to function while under cyberattack. While this approach does not provide training under all possible cyberattacks, it does allow a broad range of attacks that mitigates the previously identified concerns. The paper provides an expanded rationale for adding cyberattack effects, explaining what attacks and actions are possible and how we have imposed them in C2SIM.

**Introduction**

Cyber security is recognized as a major mission domain by the United States Department of Defense [1] and has become a major concern in military operations. This implies a need for 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. This paper applies to the latter, which is quite important because military forces must be prepared to function effectively in such an environment. In the remainder of this paper we will explore that need and then describe a technology, command and control (C2) – simulation interoperation (C2SIM) [2] that we are expanding to demonstrate a promising approach to providing such training. The paper also describes our first practical trial uses of C2SIM for training in a cyber-active environment, in NATO CWIX 2017 and 2018, and concludes with a view toward the future of this approach.

**Importance of operational training under cyber-active conditions**

> *"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 [3]*

Generally speaking, cyber-related training has two distinct audiences: 1) training cybersecurity technical personnel to provide for defense (and possible offense) for operational systems and 2) preparing operational military organizations to function effectively in such an environment.

Recently there has been great deal of focus on the former, with a continued assessment [4] that US DoD systems remain susceptible to cyber-attacks. A priority effort of the US Department of Defense (DoD) is the development of a Persistent Cyber Training Environment (PCTE) [5] that supports cyber mission force (CMF) training (also known as cyber-for-cyber). The initial development and employment of U.S Army cyber mission teams that are certified at the individual and collective level is nearly complete [6] and maintaining the readiness of these teams begins in earnest in 2018. The PCTE supports the training requirements of these team. A different example of a modeling and simulation (M&S) capability to support personnel training is the Network Effects Emulation System (NE2S) [7] that provides a realistic emulation of network and host-based cyber-attacks to integrate traditional test and training environments with cyber-attack scenarios with centralized control of real-time, instructor-initiated effects, or scripted scheduled scenarios [7].

To date, there has been less focus on providing training tools that support training operational military units in cyber-active environments. Cyber-for-leaders and cyber-for-all training is necessary to allow Army, Joint, and Coalition forces to be successful in Unified Land Operations (ULO) by effectively

integrating cyber, signal, electronic warfare, intelligence, information operations, and space capabilities to ensure cyber domain dominance while concurrently forbidding the advantage to their adversaries [1]. To implement ULO there must be effective training of coalitions in cyber-active environments. Leaders, staffs, and units must prepare for ULO envisioned military operations during training by employing CEMA enablers and support systems during collective training and unit exercises [8] just as they will during military operations. Future military operations will be conducted in a highly contested cyber-active environment; military organizations must begin training now to work with degraded information systems and even with no systems at all [9].

Using a "crawl-walk-run" model of training, decoupling cyber aspects of ULO is desirable during the early *crawl* phase as personnel are learning their baseline non-cyber skills, perhaps through the use of a small-scale table-top exercise or similar construct to practice key process and procedure changes [10]. During the ensuing *walk* phase, cyber concepts and effects must be introduced in order to prepare military personnel for the *run* phase. This last phase of 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 [10].

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 Cyber tool 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.

**C2SIM background**

The vision of C2SIM is that future military coalitions will be able to train together simply by plugging their C2 systems and simulations into a common network and using open, consensus-based standards. A series of three numbered Technical Activities in the NATO Modeling and Simulation Group (MSG), has resulted in growing recognition of the need for C2SIM. NATO MSG-048 demonstrated technical feasibility of C2SIM (at that time called Battle Management Language or BML) [11]. MSG-085 confirmed military utility by demonstrating a coalition of six national C2 systems and five national simulation in a distributed mission planning exercise [12,13].

Figure 1 shows the architecture of the successful system of systems demonstration conducted by MSG-085 at Fort Leavenworth, Kansas in 2013. The demonstration included interoperating servers from two nations and operations distributed to Madrid, Spain and Farnsborough, UK in addition to the main site at Fort Leavenworth, Kansas. This demonstration resulted in firm recognition of the military utility of C2SIM. In its aftermath, MSG-145 currently is pursuing operationalization of C2SIM along with its adoption as a standard, first in the Simulation Interoperability Standards Organization (SISO), then by NATO as a Standardization Agreement (STANAG).

Technical development and military evaluation by NATO must be complemented by industry-based standards development. The existing first-generation BML standards are Coalition Battle Management Language (C-BML)[14] and Military Scenario Development Language (MSDL)[15]. Product Development Groups (PDGs) for both of these standards had planned a second generation; at the recommendation of MSG-085 the groups came together as the C2SIM PDG with the goal of integrating initialization, tasking and reporting in a single standard that would be extensible in order to minimize complexity [16,17]. The C2SIM standard draft and ontology currently are nearing completion by the SISO C2SIM Product development group.

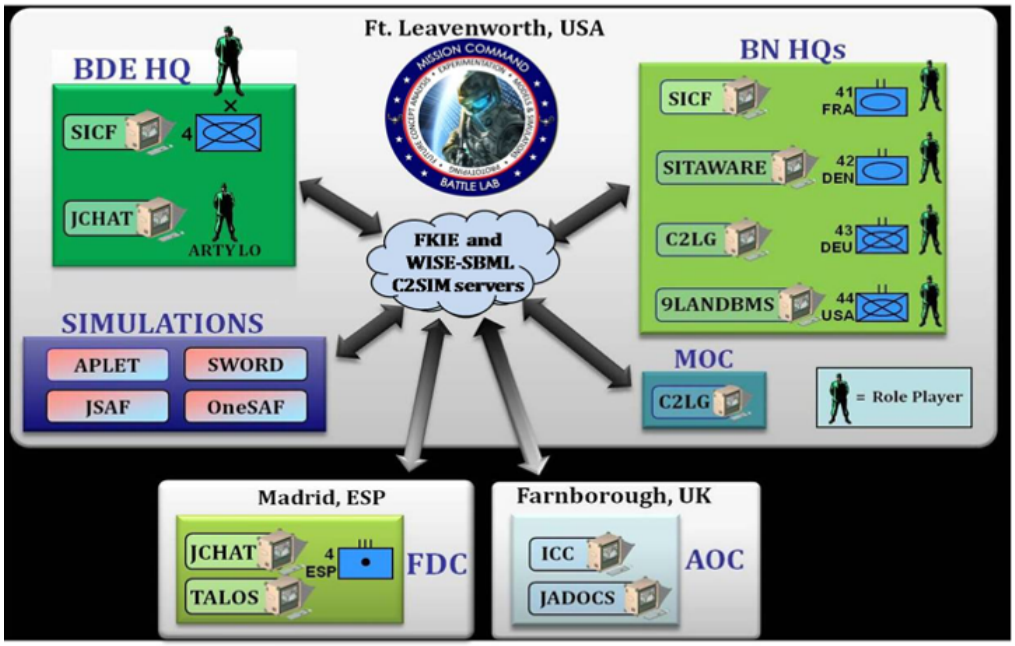


**Figure 1: Architecture of C2SIM system-of-systems demonstration**

**C2SIM Reference Implementation Server**

The general architecture for C2SIM is shown in Figure 2. The C2 systems interoperate among themselves using their own standards while the simulation systems interoperate among themselves using their own standards. C2SIM provides for exchange of C2 information (order, requests, reports) within this system of systems. The role of the server is to distribute the orders, requests, and reports among the C2 and simulation systems on a publish/subscribe basis.

The C4I and Cyber Center at George Mason University has produced a sequence of servers to support the progress of the NATO MSG activities. The final demonstration of MSG-085 used distributed servers to provide more processing power and communication efficiency. As shown in Figure 1, the system was heterogeneous, consisting of the FKIE server from Fraunhofer FKIE and the WISE-SBML server from Saab Corporation and George Mason University (GMU) [18]. Because development had proceeded piecemeal before availability of the VPN testing environment, four related but different schemata were potentially in use. The FKIE server supported an FKIE-extended “IBML09+” version of the schema from MSG-048 [19], while the WISE-SBML server supported, and could translate among, IBML09, IBML09+, and the two

subschemata of the SISO C-BML standard (although, as it turned out, only the "light" version of C-BML was used). Translation required that the WISE-SBML server parse each C-BML order and report and reformat them to comply with the various schemata. Such complexity would have been unsupportable during MSG-048, four years earlier.

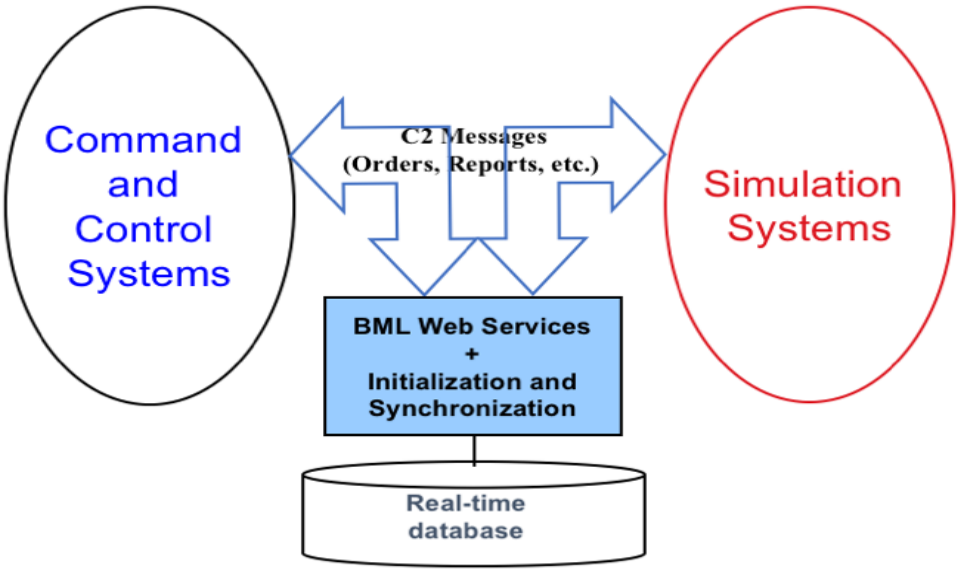


**Figure 2: General Architecture for C2SIM**

The latest server from GMU is the C2SIM Reference Implementation Server. It is written in Java for ease of understanding and portability and translation, like that of the WISE-SBML server, that will be used allow backward compatibility of C2SIM with MSDL and C-BML but is not intended to support a very high message rate. It implements the standardized C2SIM messages and initialization semantics of the draft SISO C2SIM standard and translates them to and from IBML09 and C-BML for backward compatibility. It also features logging and replay, late joiner support and checkpoint/restart; and it is available as completely open source software.

**Cyber effects editor**

Our latest work makes it possible to apply many of the effects of cyber and electronic warfare attacks by modifying the C2 messages that flow through the C2SIM server, as shown in Figure 3. The significant difference between Figure 2 and Figure 3 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 [7,10] and the US Army's OneSAF prototype Cyber Operations Battlefield Web Service (COBWebS) [20]. In each of these systems, all effects have been imposed in a single simulation. Thus, it was not possible to emulate cyber effects in associated C2 systems, in the supporting network, or in various members of a coalition of such systems operating under the MSDL/C-

BML standards. By imposing cyber effects in the simulation, it is possible to achieve a wide range of training stimuli across a coalition without compromising and C2 systems or adding functionality to simulation systems. This can be achieved in environments as simple as a single pairing of C2 and simulation, more complex environments such as in joint training with each component having its own C2 system and simulation, or the even more complex environment in a coalition where several nations are involved, each with one or more C2 systems and simulations.

As shown in Figure 3, the modified 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 as part of operational testing carried out by NATO MSG-145 in the Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (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.

The Cyber Effects Message Editor is capable of imposing the following effects on order, request and reports passing through the Reference Implementation server. The general categories of action are electronic warfare (EW) where messages are dropped and cyber attacks where messages are modified. We expect to add more of the latter, as experience is gained with these:

*Electronic Warfare*

- block a specified fraction of messages for a specified duration
- block a specified fraction of messages at random intervals, off and on times both uniformly distributed, with separate on and off mean specified
- block every nth message for a specified n
- block all messages from specific area (“blanket” jamming) for a specified duration

*Cyber attacks*

- modify all reported locations by a specified (lat,lon) offset
- modify report time by a specified (seconds, minutes) offset
- block all messages from a specified device simulated device
- block all message from a specified C2 system

*Implementing actions on receipt of a C2 message*

- process the message normally
- modify the message and then process it normally
- drop the message

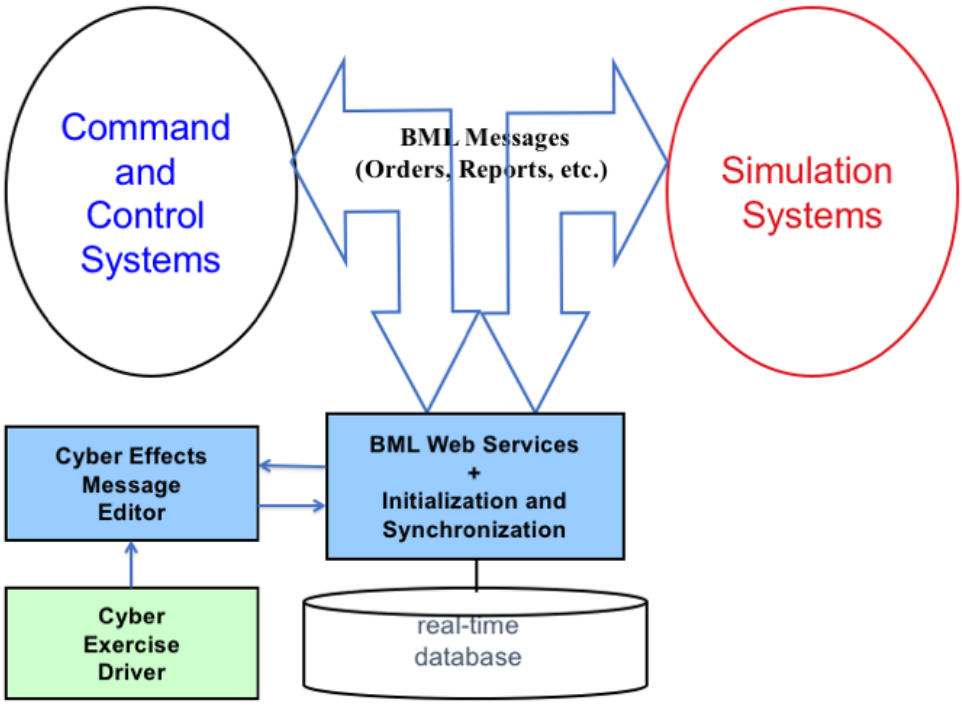


**Figure 3: C2SIM architecture with cyber effects Imposed on C2 messages**

**Using cyber effects in CWIX 2018**

The C2SIM Cyber tool mitigates the risk of disruption and readiness by introducing cyber-attacks at the C2SIM server. This allows a controlled environment to be established that allows the unit to include cyber events as their training level allows and has no damaging impact on the readiness of C2 assets and provides a significant improvement over the main method currently used. The most common current training methodology entails use of manual workarounds known as "white cards" by exercise controllers to inject rudimentary degraded or denied conditions into exercises which are typically low fidelity and have little or no relation to ongoing cyber effects [10]. This is a less effective method of training than having systems users directly identify potential cyber threats and take effective action to reduce or eliminate the threat. "White cards" may support training during *crawl* and *walk* phases of training but due to the deviation from "train as you fight" they have a negative impact on training during the *run* phase.

As an even more primitive alternative, it is possible to measure the success of implementing an EW jamming threat or cyber denial of service threat into a training event by terminating information flow. This is what would happen due to the collapse of effective communication. In effect, the training audience loses the capability to achieve any objective due to an inoperable communication and network capability. However, most exercise designers would not agree to a sufficiently robust implementation of a cyber threat that would halt their exercise.

Determining the impact of an introduced cyber threat to the training audience requires a well thought-out and resourced observation plan that knows when the threat was introduced couple with what impact results and identifies when users recognize the threat and take action to mitigate its impacts. As

with any tool, the objectives of the training event must be set then the tools identified that will help the training audience achieve the objectives. The overarching objective of executing cyber training scenarios that involve multiple entities is to ensure that systems (information systems, networks, connected devices) users successfully react to cyber effects during the exercise scenario.

The Cyber Effects Message Editor operates with C2SIM, which is one of the few simulation tools designed to operate in a coalition context with the Army's Unified Action Partners (UAP). This environment is difficult to maintain due to the inherent differences of national policies, which is extremely complex when it comes to cyber. C2SIM and its cyber tool allow each nation to train on its own systems with its own policies in place, negating the requirement for an overarching agreement on how cyber effects will be dealt with. In effect, the C2SIM Cyber tool injects the cyber effect at the C2SIM server and the results are implemented on each nation's C2 system via their own simulation system. The training audience then handles the cyber effect in accordance with their own nation's policies and per coalition agreements.

This approach will provide meaningful training for cyber-for-all and cyber-for-leaders training audiences. These audiences will be faced with cyber activities that they will have to react to during the normal operation of their C2 system as well as work through the threat in a coalition environment. Cyber-for-cyber (or Cyber Mission Force (CMF) are not training audiences here, as they would receive less meaningful training since the C2SIM Cyber tool will only emulate the effects on network devices; it will not allow them to be reconfigured/replaced to eliminate threats. Thus, the training benefit for Cyber-for-cyber is reduced to their key task of advising leaders on actions to take.

In the initial evaluation during CWIX 2018, C2SIM CEMA effects were tested as part of the first major tests of C2SIM. 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 [21]. 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.

However, CWIX 2018 was only an initial technology test. 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. But 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.

**Conclusions and Future Work**

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 intense test, including human role-players and additional cyber behaviors is planned for 2019. Testing

will deny (block all messages related to a particular operation), degrade (random dropping of messages during set or random periods), disrupt (drop message bits at various levels of magnitude or change messages), and prevent (inhibit GPS and other prevent supporting services/devices). Other possibilities include adding a scripting option to trigger activity within one or more simulations, such as an order to shut down communication capabilities represented within the simulation.

Cyber-for-cyber (CMF) training will continue to be the responsibility of each nation in a C2SIM supported event. The C2SIM Cyber tool supports cyber-for-others (leaders) and cyber-for-all (C2 system operators) in order to prepare them and the coalition that they operate in cyber threats and conducts successful military operations in a cyber-active environment.

**References**


[1] U.S. Army Cyber Center of Excellence Strategic Plan, September 2015, https://cybercoe.army.mil/images/CyberCoE%20Documents/strategic_plan_2015_revision4_9_14_2015.pdfdownloaded 22 May 2018.

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

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

[4] www.dote.osd.mil/pub/reports/FY2017/pdf/other/2017cybersecurity.pdf, DOT&E FY 2017 Annual Report, downloaded 22 May 2018.

[5] Project Manager Instrumentation, Targets, Threat Simulators, and Special Operations Forces Training Systems Overview, http://peostri.army.mil/tsis17_itts_final, downloaded 25 May 2018.

[6] U.S. Army Public Affairs, Cyber Mission Force achieves full operational capability, May 18, 2018, https://www.army.mil/article/205585/cyber_mission_force_achieves_full_operational_capability, accessed 25 May 2018.

[7] 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.

[8] U.S. Army LandCyber White Paper 2018-2030, 9 September 2013, http://dtic.mil/dtic/tr/fulltext/u2/a592724.pdf downloaded 22 May 2018.

[9] Seffers, G., Army officials outline challenges to cyber, signal and electronic warfare training, Signal, 9 August 2017, https://www.afcea.org/content/training-cema-force, accessed 25 May 2018.

[10] 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.

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

[12] Burland, B., J. Hyndøy, and J. Ruth, "Incorporating C2--Simulation Interoperability Services Into an Operational Command Post," International Command and Control Research and Technology Symposium 2014, Alexandria, VA

[13] Khimeche, L., M. Pullen, R. Wittman, B. Burland, J. Ruth and J. Hyndøy, "Coalition C2-Simulation History and Status," NATO Modelling and Simulation Symposium 2014, Washington, DC, October 2014

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

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

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

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

[18] 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

[19] 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

[20] 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

[21] 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