Introducing Cyber Effects in C2 Simulation

Dr. B. Boltjes[1], Dr. M. Pullen[2], Dr. K. L. Morse[3]
[1]TNO Defence Research, The Netherlands
[2]George Mason University, C4I Centre.
[3]Johns Hopkins University / Advanced Physics Laboratory

Abstract — Force readiness (education and training), execution and support to operations (planning, mission rehearsal, control of autonomous systems) and Defence Acquisition (capabilities development, systems qualification) heavily lean on C2 to simulation interoperability. To enable information exchange in a timely, efficient and cost-effective manner in turn requires a standardized representation and interfaces that allow Command and Control (C2) and simulation systems to interoperate. The C2SIM standard that is being developed for that aim. Effects of cyberattacks and the ability to perform counterattacks should be represented in this. However, there is currently little representation of cyber in campaign and mission level exercises, what there is being mainly limited to degrading or switching off C2 systems or simulators. Although this can be a quick and effective way of creating a basic representation of the impact on a mission of a cyberattack, it does not cover the full range of potential impacts. This paper shows possible paths to more effective representation of cyber effects.

1 INTRODUCTION

This paper describes the cooperation between people, nations, and Cyber Modelling and Simulation (M&S) technologies. It describes standardization and design activities, identifies synergies and progress in simulating cyber effects in mission training and exercises.

2 MSG-170

The current NATO Modelling and Simulation Group (MSG) number 170 is a specialist team to produce a "top ten" list of cyber effects / attacks / countermeasures and countereffects that are most worth modelling. This technical activity follows on from the work of MSG-117 and the MSG-151 workshop that reported in 2015 and 2017 respectively. The report published by MSG-117 gave an informed high-level overview of how M&S might be used to support NATO Cyber Defence efforts [2]. One of the most significant areas identified as needing additional work to ensure the potential of M&S to support this domain is fully exploited was the representation of the impact of cyber in training exercises for military personnel other than cyber operators. Possibly informing NATO on the requirements for a NATO Cyber High Level Architecture (HLA) Federation Object Model (FOM) module. The envisioned "top ten" list of MSG-170 would be exploitable across a range of follow-on and related M&S activities. One such related activity is the Simulation Interoperability Standards Organization (SISO) C2SIM product development group which explores how to introduce these cyber effects via their C2SIM Server in cooperation with NATO MSG-145.

3 C2SIM

The C2SIM product development can use the output of MSG-170 to focus the development of standards, methods, and architectures. The goal of MSG-145 is to stimulate a standards-based NATO capability where national elements of multinational formations will be supported by their own national command and control (C2) systems and represented by their national simulations that incorporate national doctrine, equipment, and staffing. The NATO interoperability standard for C2SIM is being developed within the mandated MSG-145 task group as a STANAG that wraps the SISO C2SIM standard.

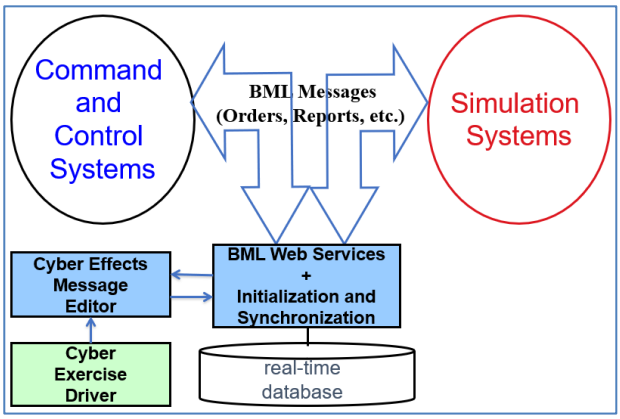

Figure 1 Introducing cyber effects into C2SIM systems

3 SISO Cyber M&S Study Group

The SISO Cyber M&S Study Group (SG) [1] is working to document ideas and experiences with cyber M&S in the form of best practices. The SG will be an important resource for early adopters of cyber M&S, lowering the barrier of entry, reducing risk, and providing guidance and support along the way. The SG's scope specifically includes efforts to:

1. Catalog, describe, and analyze current cyber M&S activities, identifying the advantages and disadvantages of each approach.
2. Conduct a literature review of SISO papers and other literature on cyber M&S.
3. Provide emerging guidance, resources and support to practitioners.
4. Investigate the potential for standards to support cyber M&S.

5. Demonstrate cyber M&S capabilities.

The group is collecting use cases and requirements for a Cyber Reference Data Exchange Model (CyRDEM), an architecture-neutral, runtime data exchange model, to determine if a standard for interoperability by design is feasible.

4 Joint Effort

This paper describes the cooperation between people, nations, and cyber M&S technologies. It describes standardization and design activities, identifies synergies and progress in simulating cyber effects in mission training and exercises.

Common identified areas of work:

1. Cyber glossary, taxonomies, and ontologies
2. Initial NATO Cyber HLA FOM module to exchange simulation information based upon the SISO Cyber Reference Data Exchange Model (CyRDEM).
3. Demonstration of cyber M&S capabilities
4. Identification of use cases suitable for development
5. Reference examples and/or available implementations

The cooperation further extends to the exchange of knowledge on existing and relevant standardization efforts and organizations, literature and vendors. Together the efforts consist of a large network of researchers in many nations. They not only work for defense, research and consultancy organization, but also for vendors with expertise in:

- M&S
- Cyber
- Cyber simulation
- M&S architectures
- Cyber training
- Cyber test and evaluation

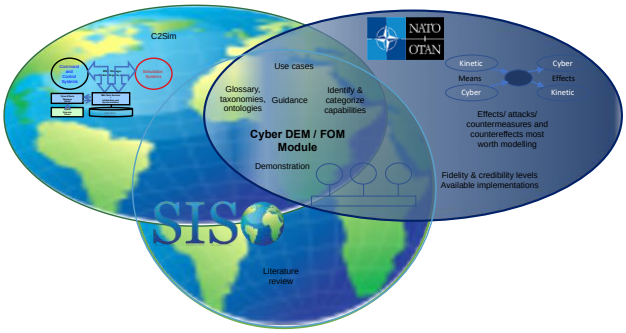

Figure 2. Joint effort intersection

This joint effort strives to improve interoperability along many axes including cyber – kinetic simulations, different cyber blended simulation capabilities, and between organizations and coalition partners.

Acknowledgements

Dr. Morse's participation in the SISO Cyber M&S SG is funded by the US DoD Test Resource Management Center (TRMC) under Contract N00024-13-D-6400.

References

[1] SISO, "Terms of Reference for the Cyber Modeling and Simulation Study Group," SISO-TOR-026-2018, 4 January 2018.

[2] "Modelling and Simulation for Cyber Defence", Final Report of Task Group MSG-117, STO-TR-MSG-117 2015.

Author/Speaker Biographies

Dr. BERT BOLTJES is a specialist in modelling and simulation with a background in physics, quantum molecular dynamics and computer tomography. For TNO in the Netherlands he has worked for EU (project Driver), NATO (MSG-117 and MSG-170), the Dutch DoD, and defence industry on performance analysis and prediction of fixed and wireless defence communication networks. He has designed, implemented, and validated high fidelity network and radio propagation models. He is a skilled in implementing technologies to couple network simulators to other simulators, hardware and live networks. Dr. Boltjes is currently performing research in M&S for Cyber, and distributed mission training with multiple levels of security.

Dr. MARK PULLEN is Professor of Computer Science and Director of the Center of Excellence in Command, Control, Communications, Computing, Intelligence (C4I) and Cyber at George Mason University. Previously he managed Internet and Distributed Simulation programs at DARPA and was an Associate Professor of Electrical Engineering at the US Military Academy West Point, NY. He serves as Co-Chair of the SISO Product Development group for C2SIM. Dr. Pullen is a Fellow of the IEEE, Fellow of the ACM, and licensed Professional Engineer. He was a leader in the team that received the NATO Scientific Achievement Award for 2013 and has had a significant role in NATO MSG-048, MSG-085, MSG-145 and in MSG-145 C2SIM testing at NATO CWIX 2017 and 2018.

Dr. KATHERINE L. MORSE is a member of the Principal Professional Staff at the Johns Hopkins University Applied Physics Laboratory where she researches, designs, develops, and applies technologies for improving simulation engineering, implementation, and application. She was previously a Technical Fellow and Assistant Vice President of Technology at SAIC. She received her B.S. in mathematics (1982), B.A. in Russian (1983), M.S. in computer science (1986) from the University of Arizona, and M.S. (1995) and Ph.D. (2000) in information & computer science from the University of California, Irvine. Dr. Morse has worked in the computer industry for over 35 years, more than 15 of them contributing to open

international standards. Dr. Morse has made significant contributions to nearly a dozen international standards, including leading the development of the Federation Engineering Agreements Template (FEAT) standard. She has served in multiple leadership positions in the Simulation Interoperability Standards Organization (SISO). She was the federation engineer for the Cyber Operational Architecture Training System (COATS). She is a member of Phi Beta Kappa, Dobro Slovo, ACM, and a senior member of IEEE. Dr. Morse was the 2007 winner of the IEEE Hans Karlsson Award.