Fortifying the Virtual Battlefield: Integrating Cyber Effects using Simulation

Matt Smith
Defence Science and Technology Laboratory
Fareham, Hampshire, UK
mcsmith2@dstl.gov.uk

ABSTRACT

Cyberspace underpins all aspects of all modern military operations, across all domains. Therefore, it is paramount that we maintain and grow our capability to conduct defensive cyber operations to prevent, nullify or reduce the effectiveness of adversary actions to preserve our freedom of action during operations. In order to prepare future forces, it is critical that the effects of cyber are accurately represented in future synthetic training systems.

Several individual activities commissioned by the UK Defence Science & Technology Laboratory (Dstl) have demonstrated how it is possible in theory to represent and distribute cyber effects in a synthetic environment. This paper describes the creation of a Cyber Effects Technology Demonstrator, which has integrated existing tools to demonstrate a combined approach.

The Cyber Effects Technology Demonstrator sought to investigate concepts for replicating realistic cyber effects in virtual & constructive simulations using open standards. During its development it was essential that open standards were used to support reuse of existing models and ensure value for money for defence.

This paper explains how an existing interoperable simulation architecture, using High Level Architecture (HLA), was expanded to include the Simulation Interoperability Standards Organisation (SISO) Cyber Data Exchange Model (DEM). This enables incorporation of existing cyber products including an adversarial emulation framework and a cyber-system simulation into a HLA federation where effects (e.g. system performance) can be observed through two commonly used COTS simulation products.

This technology demonstrator has identified an existing capability gap in the simulation of cyber effects in distributed simulation and engaged multiple industry partners to collaboratively deliver the demonstrator which has developed Cyber DEM capability in UK industry. The technology demonstrator was successfully presented to stakeholders where they were invited to discuss how Cyber DEM could be utilised in a training context.

Findings will identify challenges and lessons to provide an evidence base to support both future advice and guidance to the UK Ministry of Defence as well as contributing to a NATO Modelling and Simulation Group (MSG) task group focused on the modelling of cyber domain entities and events within distributed simulations. The task group will also provide recommendations to the SISO Product Development Group and in turn, this research will contribute to the future development of the Cyber DEM standard.

ABOUT THE AUTHOR

Matt Smith is a Senior Analyst at the UK Defence Science and Technology Laboratory. He graduated from Staffordshire University in 2015, with a Bachelor of Science with Honours in Games Design, where he specialised in virtual training simulation and realism. Since joining Dstl in 2018, his work has focused on the representation of the future operating environment for training simulation including urban operations, space, cyber, human behaviour representation and multi-domain operations.

DSTL/CP160489

Fortifying the Virtual Battlefield: Integrating Cyber Effects using Simulation

Matt Smith
Defence Science and Technology Laboratory
Fareham, Hampshire, UK
mcsmith2@dstl.gov.uk

INTRODUCTION

Cyberspace underpins all aspects of all modern military operations, across all domains. Therefore, it is paramount that we maintain and grow our capability to conduct defensive cyber operations to prevent, nullify or reduce the effectiveness of adversary actions to preserve our freedom of action during operations. In order to prepare future forces, it is critical that future training can match the character of the likely operating environments as closely as possible. (Development, Concepts and Doctrine Centre, 2022)

Cyber representation for training can be broken down into two broad areas (Couretas , 2019):

1. **Cyber for Cyber (C4C):** the representation of cyber for training for cyber personnel is task orientated and covers the tools, techniques and procedures (TTPs) use in cyber defence;
2. **Cyber for Others (C4O):** the representation of cyber effects on non-cyber personnel is impact orientated and facilitate consideration of the measures needed to minimise the effects of a cyber-attack on a mission;

In addition, and particularly at Joint and Coalition a third area is becoming of ever increasing importance:

3. **Cyber For All (C4A)** – Integrating existing cyber range environments, traditional simulation architectures, operational networks, and cyber emulations to deliver realistic cyber effects to the entire battlestaff (Wells & Bryan, 2015).

Naturally, these groups have differing requirements when it comes to the fidelity and classification of the training. The subject of this paper is a technology demonstrator, whilst the primary consideration is how a technology could be applied to support collective training for non-cyber war fighters and explore the appetite for a C4A approach, the research did not exclude the considerations of C4C training.

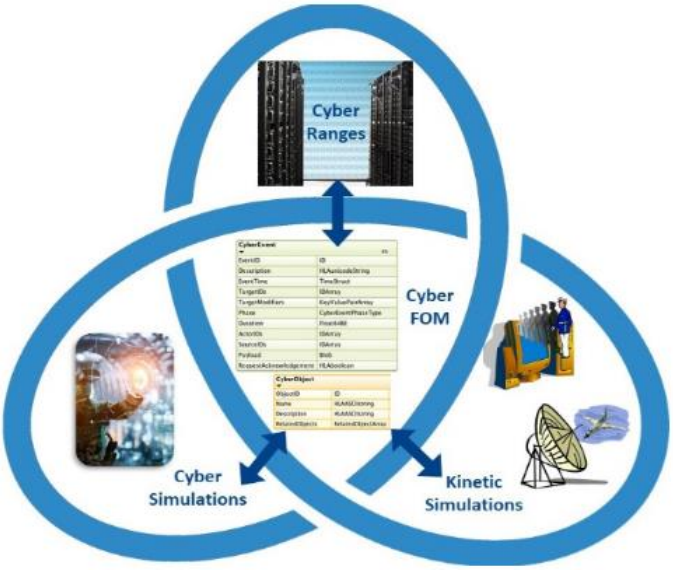

Figure 1: Draft of an HLA Cyber FOM based on the SISO Cyber DEM

The Defence Science & Technology Laboratory (Dstl) Developing Education, Training and Learning Advances (DELTA) project commissioned three studies through a Cyber Security Pitch Panel. The individual studies, demonstrated that it was possible in theory to represent and distribute cyber effects in a synthetic environment. These studies included:

1. Study 1: An investigation into the recently published Simulation Interoperability Standards Organisation (SISO) Cyber Data Exchange Model (DEM);
2. Study 2: Adding simulated agents to an existing Cyber Vulnerability Assessment tool;
3. Study 3: Integrating an adversarial emulation framework with virtual simulation.

The Cyber Effects Technology Demonstrator sought to investigate concepts for replicating realistic cyber effects in virtual & constructive simulations using open standards. This enabled previous study 1 to be built upon by integrating the outputs from studies 2 and 3.

This paper explains how an existing interoperable simulation architecture, using High Level Architecture (HLA), was expanded to include the Cyber DEM. This enabled the incorporation of existing cyber products including a cyber-attack simulation (study 3) and a cyber-system simulation (study 2) into a HLA federation where effects (e.g. system performance) can be observed through virtual and constructive simulations.

METHODS

The Cyber Effects Technology Demonstrator was loosely structured around Distributed Simulation Engineering and Execution Process (DSEEP), ensuring a systematic approach to the development and execution of the technology demonstrator.

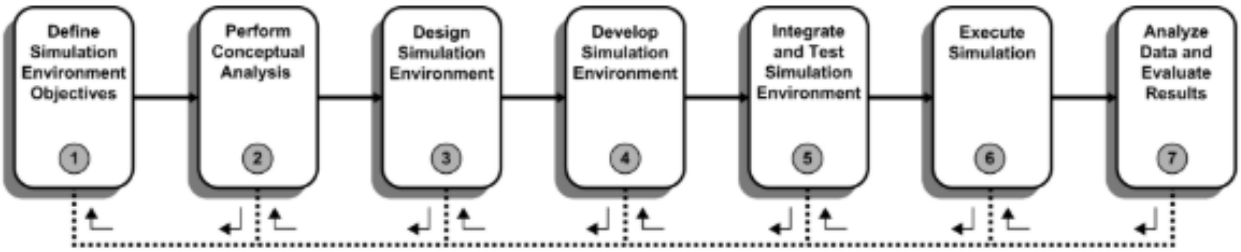

Figure 2: Distributed Simulation Engineering and Execution Process (DSEEP), top-level (IEEE, 2022)

The seven stage process as outlined by the DSEEP guidelines (Figure 2) serves as a useful framework to describe the demonstrator.

Cyber Testbed Objectives

The primary objective of this study was to demonstrate the ability to represent a cyber-effect across multiple distributed simulation federates, this ultimately enabled exploration of the potential approaches to representing cyber effects in training. Secondary objectives included identifying any limitations in CyberDEM and gaining a greater understanding of how cyber effects propagate through the simulation. The aim of this project is not to create a demonstrator that meets a particular training need but to investigate how cyber effects can be represented in simulated environments. In turn this will support stakeholders in understanding how cyber effects might be introduced into specific training systems and will provide a base to support future advice and guidance.

Conceptual Analysis

Conceptual Analysis comprised of two main elements: Conceptual Modelling and Scenario Design. The scenario was carefully designed to ensure it would effectively challenge both the representation of cyber within the individual federates and the CyberDEM as a medium for communicating them.

The concept of the demonstrator was to show how a red cyber-attack federate could attack a separate blue computer network federate. In turn this would demonstrate an effect on an associated blue system in a physical domain simulator (as shown in Figure 4).

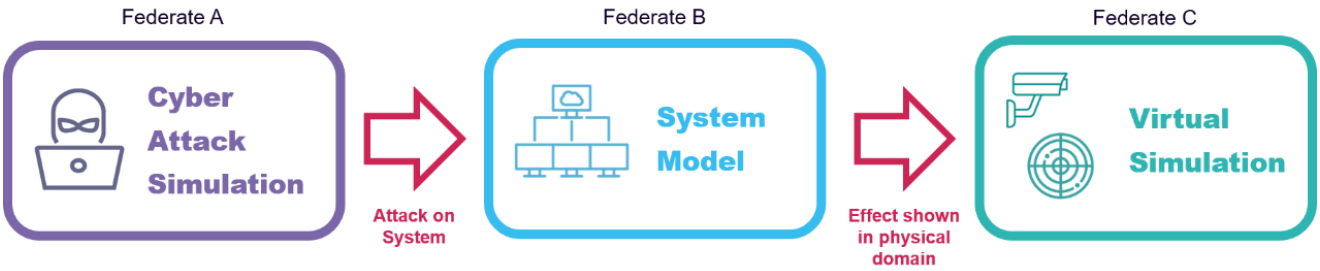

Figure 3: Cyber DEM Technology Demonstrator Concept

The scenario narrative was designed to include a wide range of effects, including:

- Deliberate and accidental GPS Jamming
- Deliberate and accidental Radio Frequency (RF) Jamming
- Data-links degradation (e.g. degradation of situational awareness via disruption to Radar/CCTV feeds)
- Information Exfiltration
- Phishing Attack

Due to project constraints only two vignettes were able to be taken forward. The vignettes, focusing on RADAR and CCTV systems, are similar in the sense that they both involve the degradation of data links however they have different methods of adjudicating whether cyber events are successful. Both methods focus around which nodes on the network (Cyber System Simulation) are accessible to the attacker (Cyber Attack Simulation). A full list of the simulation federates is detailed on page 5.

The RADAR vignette demonstrates representation of cyber effects across multiple federates, with cyber attacker, cyber defender, system model and physical domain federates.

This is a simple approach where, the Cyber Attack and Cyber System Simulation rely on their internal states and *CyberAcknowledge* interaction responses (including the *TargetID* parameter) to keep track of which devices on the network are available to be attacked. This allows federates to encapsulate their modelling responsibilities without having to rely on external systems. Attack steps are described solely by the series of interactions (*CyberAttack, CyberRecon, CyberEvent*, etc.) and their success or failure depends solely on the set parameters.

The CCTV vignette demonstrates representation of cyber effects across a network consisting of multiple federates, The CCTV system is modelled by the Cyber System Simulation, with a separate WiFi federate modelling part of the network used by the CCTV system, and a virtual simulation, Virtual Battlespace 4 modelling one of the CCTV cameras.

This is a more complex approach where the WiFi Federate publishes *PhysicalNetworkLink* objects, whose *NetworkInterfaces* attributes are updated to reflect the current state of the attack. These objects define which devices on the network are exposed to the attacker. Success and failure now depends, not only the parameters of individual interactions, but on persistent cyber objects which are exposed to the federation execution. This exposure of the current state of the attack steps allows for greater visibility, and can become even more helpful in recordings of the data and After Action Review (AAR).

Simulation Environment Design

The Cyber Effects Technology Demonstrator was designed to bring together the outputs of three separate cyber simulations studies (studies 1-3) in to a single technology demonstrator, whilst also both developing new Cyber DEM federates and integrating existing Commercial Off The Shelf (COTS) tools.

The demonstrator HLA federation used Pitch Run Time Interface (RTI) running Real-time Platform Reference (RPR) Federation Object Model (FOM) & the Cyber FOM derived from CyberDEM. An outline of this federation can be seen in Figure 4.

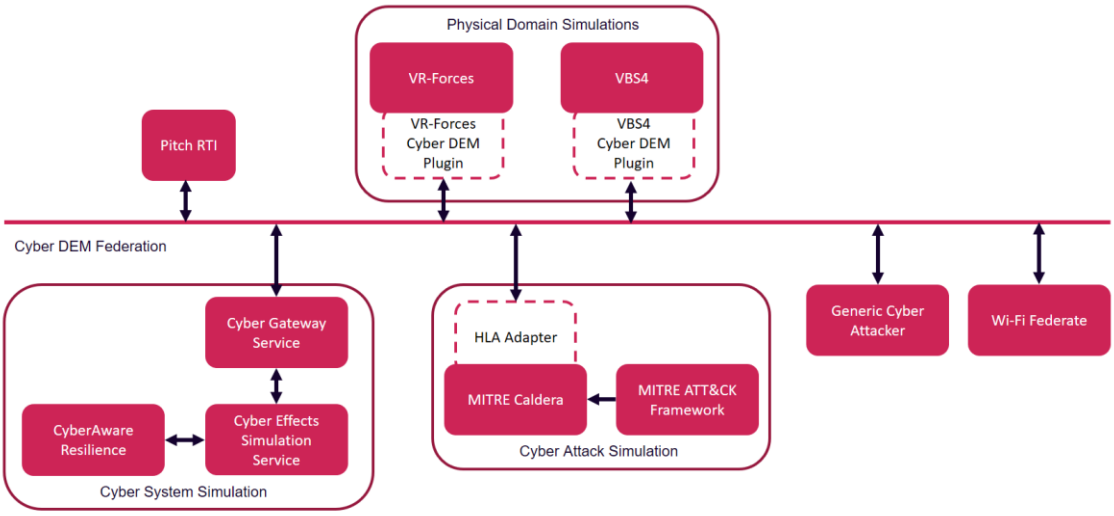

Figure 4: Cyber DEM Technology Demonstrator Simulation Architecture

The federation consisted of the following federates:

- Cyber Attack Simulation: This federate is responsible for modelling cyber-attacks. It uses tactics, techniques and procedures from the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework (The MITRE Corporation, 2013) as the basis for attacks on networked systems. It also uses MITRE Caldera as a configured adversarial framework to simulate the outputs of a cyber-attack.

- Cyber System Simulation: This federate is responsible for modelling cyber systems and cyber effects and is composed of several components:
    - CyberAware Resilience (CAR) is an 'off the shelf' product developed by RiskAware. Originally developed as part of Dstl's Joint User Mission Planning for Cyber and Electro-Magnetic Activity (JUMP) programme. It was created to provide cyber risk modelling that can be incorporated within military mission planning.
    - Cyber Effects Simulation Service (CESS) was developed under the preceding study 2. CESS is an Application Programming Interface (API) to allow a developer to utilise the underlying capabilities within CAR
    - Cyber Gateway Service has created mappings of the CAR data models to the CyberDEM standard to translate CyberDEM interactions and objects into parameters required by CAR. This enables CAR to receive and translate inputs and to provide outputs into a wider HLA federation.
- Physical Domain Simulators
    - VR-Forces: VR-Forces is a COTS Computer Generated Forces (CGF) product employed within the UK air synthetic training environment called GLADIATOR. Within this federation, it is responsible for the representation of physical systems, primarily air platforms and associated sensors (e.g. radar).
    - VBS4: VBS4 is a COTS virtual desktop training simulation that is widely used for land forces training under the Defence Virtual Simulation 2 (DVS2) enterprise contract which provides a virtual simulation tool to UK Armed Forces, free at the point of need. Within this federation, it is responsible for the representation of physical systems, primarily land platforms and associated sensors (e.g. camera systems).

- Cyber DEM Plugins – To support the development Cyber DEM integration, plugins needed to be developed to support integration into both physical domain simulators.

- Wi-Fi Federate – This is a new federate developed to represent a Wi-Fi hotspot. This federate demonstrated cyber events that involve both attacking and defensive measures.

- Generic Cyber Attacker – This Graphical User Interface (GUI) based federate is capable of invoking CyberDEM events and receiving CyberDEM objects and interactions. It was originally developed through the previous phase study 1 to inject CyberDEM events into traditional simulation tools.

RESULTS

Demonstration Event

The technology demonstration took place on June 18th 2024 with a range of military stakeholders and partners across government (PAG's) in attendance it was a successful event with the demonstrator running without technical issues.

Figure 5: (left) CCTV Vignette Scenario (right) View from CCTV camera inside VBS4

Following the demonstration a discussion was facilitated to understand feedback from the military stakeholders particularly in understanding use cases where they thought cyber DEM could add value to training systems.

Feedback

There was concern across a number of military stakeholders as to the suitability of current scenarios and equipment for training cyber and it was felt that integration of cyber effects using CyberDEM could be used to fill that gap. There was general agreement that systems need to allow the training audience to understand the impact that cyber has on them both in the short and long term.

There was a consensus that there is a need for cyber to be trained as part of exercises. However, there was disagreement as to how that is best achieved and some discussion of whether a 'cyber for all' approach was desirable for collective training. On one hand, some stakeholders felt that cyber ranges should be able to participate as part of joint collective training. Others felt this may detract from the existing training and separate exercising with the outputs of a higher fidelity cyber exercises being used to inform the injects and effects would be more desirable.

Lessons Identified

It was identified that there was a difference in fidelity between the Cyber Attack Simulation and the Cyber System Simulation. The Cyber Attack Simulation model, Caldera, has a much higher fidelity in how it models the attacks compared to the Cyber System Simulation model, CyberAware Resilience, which is intended to provide a higher level mission model overview of an attack. Caldera runs individual attack steps on each node whereas CyberAware Resilience is concerned with the overall progression of the attack through the network. Despite these differences, CyberDEM effectively enabled that gap to be bridged.

There was also a difference between attack steps run by Caldera and the *CyberAttack* events available in CyberDEM. In order to achieve the vignettes demonstrated, it was necessary to use *TargetModifiers* or in some cases extend the CyberDEM in order to be able to send the relevant information.

There is currently a wide range of *CyberEffect* events in the DEM and it would be useful to replicate this on the *CyberAttack* event side of the DEM. The requirement for higher levels of detail in the attack steps would depend on the audience for any particular simulation. The structure of the DEM is such that it would always be possible to abstract it back up to a higher level if that better suited the objectives of the simulation.

CyberDEM offers several customisable data fields, such as *TargetModifiers* that allow users to define and exchange data that goes beyond the scope of what Cyber DEM provides. However, when using these customisable fields, the data defined is not standardised. This lack of standardisation will make any federate using these fields harder to reuse effectively.

RECOMENDATIONS

Whilst this project successfully demonstrated the use of HLA and CyberDEM as a means to manifest the effects of cyber-attack across a simulation federation, there are several areas where further work could be done to improve either the interoperability or the overall training effectiveness.

Future CyberDEM Development

- Extension of CyberDEM to include more *CyberAttack* events**:** This study found that the CyberDEM already meets the requirements in cases where a simulation is only interested in the effects of an attack. However, it would be beneficial to supporting a broader range of cyber use cases if the CyberDEM was extended to include a wider range of *CyberAttack* events without requiring that level of fidelity to be used in every case.

- Identify commonly used *TargetModifiers* to be introduced into CyberDEM as separately defined attributes: As the *TargetModifiers* are not standardised, it will make re-use of components between different simulations difficult as interoperability challenges are likely to exist. For example, one simulation may have used a username field as key 'user' while another may have used 'credentials'. Whilst these semantically mean the same thing, they would not be understood programmatically causing interoperability issues.

Cyber Federates Development

- Develop a 'playbook' of cyber effects that training simulations need to incorporate to support requirement writing for future simulation procurements: It has been highlighted in previous work (Wells & Bryan, 2015) that when integrating Cyber DEM with existing traditional M&S tools, modifications need to be made in order to make the tools "cyber aware". This means that tools will need to be able to apply the correct effect to the Cyber DEM inputs being provided. The lack of "cyber awareness" is still a prevalent problem and software modifications need to be made to integrate existing traditional M&S tools with a Cyber DEM federation. Developing a catalogue of relevant cyber effects which need to be incorporated into virtual and constructive simulations would support the development of system requirements for future systems.

- Develop CyberDEM interfaces for a broader spectrum of adversary emulations to support different usecases: This work focussed on the development of a federate as a means to provide an HLA adapter for the Caldera adversary emulation tool. There are, however, several other adversary emulation tools that could be used instead. In Phase 1 of this work, two other adversary emulation tools, namely Atomic Red Team and Sliver, were investigated and used to run the cyberattack simulations. These alternative tools could provide a means to run alternative attacks or include a human-in-the-loop for training purposes.

Future Cyber Collective Training Research

- Undertake further research to explore where use cases exist that support a 'cyber for all' approach and provide a clear case for the training value provided and the relevant military organisation that need to address it: Whilst previous programme's such as Cyber Operational Architecture Training System (COATS) has implemented a 'cyber for all' approach and this technology demonstrator has demonstrated the potential for that to be achieved leveraging open standards, there is still some conflicting views as to the value of integrating cyber ranges, traditional simulation architectures, operational networks, and cyber emulations for the purpose of training.

- Undertake further research to understand the requirement to integrate a cyber training audience when training for multi-domain operations: Feedback from stakeholders largely limited to consideration of single domain training audiences. As allied forces implement Multi-Domain Operation warfighting concepts the consideration of where a cyber training audience may need to participate in joint training exercises alongside kinetic forces should be considered. Future research should include if and where in the training progression joint training between cyber and other domains needs to take place.

SUMMARY

The successful demonstration and collaboration with the suppliers provides compelling evidence that the use of CyberDEM is an effective means to allow the effects of cyber-attacks to be manifested across multiple simulation federates including representations of the physical domain. CyberDEM offers a standard interface, enabling each component to be replaced with one of similar functionality to achieve the same outcome. However, currently this relies on an adapter being developed as there are no COTS models which have been developed to natively interoperate with CyberDEM.

This work shows how, through the use of open standards, training platforms could begin to be used to allow military personnel to develop a greater knowledge and understanding of the effects of different cyber-attacks. This would enable them to undergo appropriate training to be able to recognise when cyber-attacks are occurring and take the necessary steps to mitigate the effects of an attack.

ACKNOWLEDGEMENTS

This work would not have been possible without the contributions made by the cross industry technical team who designed and developed the demonstrator. Additionally the documentation produced by the development team has made a significant contribution to the content of this paper.

- Julie Larkman & Chris Bugden (QinetiQ Training and Simulation)
- Jon Denny & Matt Tipper (Pitch Technologies)
- Helen Adams & Russell Mills (Riskaware)
- Samantha Huntly & Harry Neil (Montvieux)

In addition, I am grateful to Jon Farrington and Andrew Hodkinson for the development of the scenario and the capture of feedback and lessons learnt which informed the helped shape the recommendations provided in this paper.

Finally, Dr Katherine Morse and Dr Fuzzy Wells for providing direction to the previous COATS research and other reference material.

REFERENCES

Development, Concepts and Doctrine Centre. (2022). *Cyber Primer.* London: United Kingdom Ministry of Defence.

Couretas , J. M. (2019). *An Introduction to Cyber Modeling and Simulation* (1st ed.). Wiley.

Development, Concepts and Doctrine Centre. (2022). *Joint Doctrine Publication 0-01 UK Defence Doctrine.* London: UK Ministry of Defence.

IEEE. (2022). *IEEE Recommended Practice for Distributed Simulation Engineering and Execution Process (DSEEP).* IEEE.

The MITRE Corporation. (2013). *Adversarial Tactics, Techniques, and Common Knowledge ATT&CK® Framework*. Retrieved May 16, 2024, from MITRE: https://attack.mitre.org/

Wells, D., & Bryan, D. (2015). *Cyber Operational Architecture Training System – Cyber for All.* Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC).