Integrating existing Cyber Ranges and Cyber Tools into LVC Simulations

Jean Paul Dingemanse, Frank Drop,
Marieke Klaver, Veronique Marquis
TNO
The Hague, NL
jean_paul.dingemanse@tno.nl
frank.drop@tno.nl
marieke.klaver@tno.nl
veronique.marquis@tno.nl

Bert Boltjes
Dutch MoD - Defense Cyber Command
Cyber and Warfare Center
Soesterberg, NL
b.boltjes@mindef.nl

ABSTRACT

In recent years, cyberspace events, attacks, effects, and responses have been increasingly integrated into to Live, Virtual, Constructive (LVC) simulations, to raise awareness among general military personnel about the potential impact of cyberattacks on a mission. In 2024, the Simulations Interoperability Standards Organization (SISO) released the Cyber Data Exchange Model (Cyber DEM), a framework designed to support the interoperability between cyberspace models, simulations, cyber ranges involved in LVC simulations, and potentially also other cybersecurity systems. Connecting actual cyberspace elements, such as cyber ranges, can drastically improve the fidelity of simulated attacks, responses, and effects. In this paper, we investigate the fit-for-purpose of the Cyber DEM with two experiments performed within the scope of the Coalition Warrior Interoperability Exercise (CWIX) 2025. The first set of experiments involved a distributed simulation comprising of two cyber-aware simulation applications. The second set of exploratory experiments revolved around the question of how a cyber range can be effectively integrated with an LVC simulation. In this paper, we report on some initial findings. Although highly desirable, integrating a cyber range into a simulation environment can require substantial effort, depending on the chosen architecture. Since a cyber range typically comprises a broad collection of ICT systems and software, interfacing with the Cyber DEM at the individual application level could result in a large number of specific interfaces. An alternative architecture would involve integration through mediation with existing communication standards used within the military cyber security domain that also intend to describe cyberspace events, attacks, effects and responses. An initial exploration revealed two candidates. First, the NATO APP-11 Message Catalogue recently added six messages describing cyber events, observations, and responses. Second, the Malware Intelligence Sharing Platform (MISP) was recently adopted as the NATO standard for sharing threat intelligence between Cyber Security Operation Centers (SOC). In this paper, we focus our attention on the potential of the APP-11 cyber messages. The tests performed at CWIX 2025 revealed no major shortcomings in the Cyber DEM. That is, all objects and interactions that we wanted to communicate between simulation systems could be successfully described using the Cyber DEM. We also found that the information described in the APP-11 cyber messages could be transformed easily into Cyber DEM objects and interactions. The results give us confidence that more challenging use-cases involving more complex cyber interactions can be handled. Future work will focus on the integration of cyber ranges with LVC simulations.

ABOUT THE AUTHORS

Jean Paul Dingemanse is a scientist and software engineer working at TNO in the Intelligence and Decision Support department. With an M.Sc. degree in Data Science he focusses on research in artificial intelligence for decision support and Modeling and Simulation (M&S). Currently he focusses on both the M&S of cyber effects and mission management during vessel operation.

Dr. Frank Drop is a senior system engineer working at TNO, with a focus on M&S technologies and architectures. He obtained his M.Sc. and PhD degrees in Aerospace Engineering (both with a focus on control and simulation) from the TU Delft, The Netherlands. His current research interests include M&S of cyberspace, and cloud-related technologies for M&S.

Dr. Bert Boltjes is an SME in modeling and simulation in a wide range of domains. Starting in quantum physics and medical computer tomography, via data communication systems, to currently cyber. He has worked for Universities,

TNO, in EU projects, and in many NATO working groups on the M&S of cyber effects. He is currently steering the introduction of M&S of the cyber domain for training and exercises of the Dutch Armed Forces.

Dr Marieke Klaver is program manager and senior scientist at the Netherlands Organization for Applied Scientific Research TNO. She has over 30 years of experience in the research areas of cyber security and critical infrastructure resilience. In recent years she has been involved in several projects that focus on modeling and simulation in support of cyber security.

Veronique Marquis is a project manager working at TNO's Mission Simulation and Training department, leading R&D projects related to the simulation of cyber security, radio communications and quantum sensing. With an academic background in crisis management, cyber security governance, and political science, she brings over seven years of experience advancing security and digital transformation initiatives in the Netherlands and Canada.

Integrating existing Cyber Ranges and Cyber Tools into LVC Simulations

Jean Paul Dingemanse, Frank Drop,
Marieke Klaver, Veronique Marquis
TNO
The Hague, NL
jean_paul.dingemanse@tno.nl
frank.drop@tno.nl
marieke.klaver@tno.nl
veronique.marquis@tno.nl

Bert Boltjes
Dutch MoD - Defense Cyber Command
Cyber and Warfare Center
Soesterberg, NL
b.boltjes@mindef.nl

INTRODUCTION

Modeling and Simulation (M&S) is used in many domains for many purposes, including the five main domains recognized within NATO: Air, Maritime, Land, Space, and Cyber. Live, Virtual, Constructive (LVC) simulation, i.e., the combination of live, virtual and constructive elements within one real-time distributed simulation, is used primarily for Training and Education purposes. Other applications could include Concept Development and Experimentation (CD&E), mission rehearsal and decision support. Simulation is used within training exercises at all four levels of training: educational, individual, collective, and exercises. At all levels of training, there is a desire to train with effects caused by events taking place in the cyber domain. For non-cyber personnel including such cyber elements in training exercises is expected to lead to an increased cyber awareness.

Currently, few simulators provide extensive support for the cyber domain. That is, common Computer Generated Forces (CGF) simulators do not contain cyber models. Simulation tools with a wide adoption, such as Virtual Battle Space (VBS) and Joint Conflict and Tactical Simulation (JCATS), lack native support for Cyber M&S. The primary focus of these simulators remains on kinetic warfare. As a result, the cyber domain is underrepresented in mainstream simulation environments.

LVC simulations typically involve several models, hardware-in-the-loop systems, human-in-the-loop interfaces, and other systems, possibly from different vendors, that are distributed over multiple computer systems. The various systems need to interoperate with each other, for which interoperability standards for simulation are used and maintained by the Simulations Interoperability Standards Organization (SISO). Recently, SISO released a novel standard to facilitate the interoperability of simulation components simulating the cyber domain. The Cyber DEM represents cyber events and objects independent of simulation interoperability solutions, but which can be directly mapped to those solutions (SISO, 2023). Translating the Cyber DEM to the NATO standard for federated simulation, the *High Level Architecture*, results in the Cyber Federation Object Model (FOM) (SISO, 2024).

The purpose of the Cyber DEM is to facilitate interaction about cyberspace conditions "between cyber ranges, cyber simulations, and LVC environments". Currently, no known military or commercial LVC simulation products offer a rich representation of cyberspace and fully support the Cyber DEM for interoperability within federated simulations. However, solutions with partial support for the Cyber DEM do exist, such as the demonstrator realized by the NATO Modeling and Simulation Group (NMSG) 200 "Cyber M&S". The Cyber DEM enables existing commercial-off-the-shelf (COTS) solutions for cyber exercises and training to be integrated in a standardized manner.

The objective of this paper is twofold. First, we aim to investigate the fit-for-purpose of the Cyber FOM by using it within the scope of a distributed simulation involving physical and cyber elements. These elements might include physical components such as telecom towers and mobile phones as well as cyber event like simulated malware attacks and Distributed Denial of Service (DDoS) attacks. Second, we aim to explore the broader topic of interoperability between cyber ranges and distributed cyber simulations. Both objectives involve exploration and experimentation efforts performed at the Coalition Warrior Interoperability Exercise (CWIX) 2025.

The investigation of the fit-for-purpose of the Cyber FOM (first objective) is done by building a federated simulation with models and applications of two organizations (Hadean Supercomputing Ltd and TNO). Hadean provides a "Pattern of Life" simulation, which consists of a wide range of physical and cyber entities that interact in many different ways, both physically and through cyber actions. TNO provides the Entity Plan View Display (EPVD), which

is a typical “white cell” application that shows the simulation ground truth and offers various means to control and influence the simulation, such as entity creation, entity property modification, magic move, and the initiation of cyber effects and actions. In the federated simulation, the EPVD will display entities that are owned by the Pattern of Life simulation, and we will use the EPVD to initiate cyber events and attacks and observe their effects on simulated entities.

To explore the broader topic of interoperability between cyber ranges and distributed LVC simulation involving cyberspace (second objective), we discuss two high-level integration concepts (architectures) and experiment with an implementation following one of the two architectures. That is, we recognize that interoperability between cyber ranges and LVC simulation can be solved “bottom up”, i.e., by creating many dedicated interfaces between individual elements of a cyber range and the simulation, or “top down”, .i.e., by creating one generic interface between the simulation and a cyber range component whose function it is to hold a complete overview of all cyber entities, events, and actions that take place in the cyber range. Such a system could possibly be the Malware Information Sharing Platform (MISP), which is now the agreed standard for malware information exchange within NATOs Standardization Agreement (STANAG) 5660 (NATO Standardization Office, n.d.). Another potential source of information about objects and events present in cyberspace are APP-11 Cyber Messages, which could additionally be shared through MISP. In this paper, we will explore mediating APP-11 Cyber messages to Cyber FOM messages, for visualization using the EPVD.

The paper is structured as follows. The *Background* section details the important concepts relevant to this paper, such as the Cyber DEM, MISP, and APP-11. The *Federated Cyber Simulation* section describes the simulation that was built to test the fit-for-purpose of the Cyber FOM for interoperability *within* a HLA-based federated simulation. It also presents the tests and experimentation results obtained at CWIX . The section *Connecting Cyber Ranges to Cyber M&S* describes the mediation between APP-11 Cyber messages and Cyber FOM messages, and the rational for exploring this architecture including the exploration results. The paper ends with a discussion and conclusions.

BACKGROUND

The background section introduces concepts that are essential to the understanding of the remainder of the paper.

High Level Architecture (HLA)

In the domain of distributed simulation, ensuring interoperability between various systems remains an ongoing challenge. To address this issue, the U.S. Department of Defense defined the High Level Architecture (HLA) (Dahmann et al, 1997) which was eventually standardized by IEEE (IEEE, 2010). The HLA is a foundational framework that allows multiple simulation components, known as federates, to work together in a coordinated way within a larger system referred to as a federation. A FOM is a core component of the HLA because it defines a shared vocabulary used by federates to communicate data and interactions.

The Real-time Platform Reference (RPR) FOM and the NATO Education and Training (NETN) FOM are also foundational components in the distributed simulation domain and are designed in alignment with the HLA framework. The RPR FOM is a widely adopted standard developed by SISO. It serves as a reference model for simulating real-time interoperability between platforms such as aircraft, ground vehicles, weapons, and personnel (SISO, 2015). To extend the RPR FOM, the NMSG developed the NETN FOM to support higher-level simulation capabilities and interoperability, such as scenario management, tasking and simulation control (NMSG, 2020).

Connecting the cyber domain to the distributed simulation domain is a relatively new endeavor. The Cyber DEM, developed by SISO, defines a standard way to describe cyber events and objects in a format that is not tied to any specific simulation system (SISO, 2023). It enables the sharing of cyber elements between cyber ranges, simulations and test or training environments. Cyber elements like emulated detection and prevention systems or threat actors. The Cyber FOM translates the abstract definitions from the Cyber DEM and implements them in HLA specific simulations (SISO, 2024).

NATO Modeling and Simulation Group MSG-200 (NMSG-200)

The NMSG-200 developed a distributed simulation demonstrator to showcase how cyber exercises and training can be integrated with other domains in a standardized manner. As part of this effort, the NMSG-200 expert group identified NATO relevant use-cases to guide the development of the SISO Cyber DEM, aligning it with specific simulation requirements. Additionally, the group explored methods for incorporating effective and credible representations of cyber effects into training and test environments.

The NMSG-200 demonstrator consists of two tools to generate Cyber Event Commands (CEC): one developed by TNO and one by the UK based DSTL (Smith, 2024). These event commands are transmitted via the HLA Runtime Infrastructure (RTI) to the commercial CGF platform, VBS. To support this integration, a customized version of VBS was created by its vendor. This version includes a modified HLA gateway capable of interpreting the Cyber FOM, receiving cyber event commands from the RTI, and sending them to objects inside VBS which then execute the commands.

Based on the findings of NMSG-200 (NMSG-200, in preparation) the following key recommendations were made: 1) to add the Cyber FOM to STANREC 4800 covering all NATO FOMs, 2) to encourage commercial simulation tool developers to make their solutions “cyber aware” and integrate them through HLA using the Cyber FOM, and 3) continue development of the Cyber DEM based on new use cases.

Cyber range

The primary function of a cyber range is to provide an opportunity for interactive simulation of an organization’s ICT, Operational Technology, mobile or physical systems, applications and infrastructures in response to cyberattacks. That is, a cyber range typically resembles (a part of) the computer systems of an organization which can be attacked by Red Teams without causing actual harm. As such, a cyber range is typically a complex collection of technical components, that all have an attack surface.

Malware Information Sharing Platform (MISP)

The MISP is an open-source threat intelligence platform (MISP Project, 2016). The platform is designed to facilitate the sharing and storage of cyber threat information among organizations. That is, a MISP instance is typically connected to one or many other MISP instances and continuously sends and receives information from the connected instances. The usage of MISP may help to improve situational awareness, coordination of responses and enhance cyber defense strategies. MISP is one of the most widely used open source Cyber Threat Intelligence platforms (Delvecchio et al., 2025). The formats adopted by MISP are a best practice to enable greater completeness, traceability, usability and security (Ramsdale et al., 2020).

APP-11 Cyber Message Standard

The APP-11 standard controls the exchange of information within and between NATO forces by defining a library of messages and instructions for their use. The use of APP-11 is mandatory for all NATO forces exchanging character oriented messages as covered by STANAG 7149 (NATO Standardization Office, 2024). The current version of the library does not contain messages related to cyber events and other information relevant to cyber defense. A proposed set of six cyber message types is now under evaluation to be added to the message catalogue. These new messages would enable NATO partners to exchange machine readable defensive cyber information quicker and more easily, which would reduce the time that military systems are vulnerable to already discovered cyber threats.

The proposed set of Cyber Messages describe cyber event information such as attacked targets, the involved malware, cyber threats, observations, and descriptions of a response to a threat or attack. Cyber event information is used to provide a grouping of indicators for a cyber event. Malware, target, threat and vulnerability information is used to notify potential affected users and systems. Response information is used to communicate responses taken and further recommended responses to the cyber event.

FEDERATED CYBER MODELING AND SIMULATION

The first objective of this paper is to report on our efforts to evaluate the *fit-for-purpose* of the Cyber FOM within the scope of a distributed simulation. This evaluation was performed by using the Cyber FOM to interoperate between two simulation applications developed by two separate organizations without prior coordination concerning the modeling of cyberspace entities and events. That is, both applications were independently developed and implemented, and so there was no guarantee that these applications would "speak the same language".

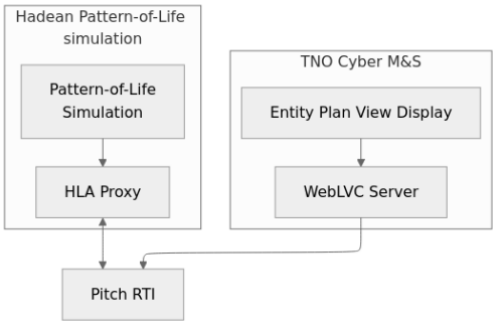

Figure 1: Federation overview

A high level overview of the federated simulation and the internal structure of each federate is shown in Figure 1. The federation contains two federates, one from Hadean and one from TNO, both connected to a Pitch RTI instance. For the Hadean Pattern-of-Life federate, a HLA Proxy translates internal data structures to the Cyber FOM types. For the TNO Cyber M&S federate, the EPVD connects to the RTI through an instance of the TNO HLA WebLVC Server. The HLA WebLVC Server is both a SISO WebLVC and HLA compliant component that enables WebLVC clients to exchange simulation data with an HLA federation in JSON format (SISO, 2022).

TNO Cyber M&S

The TNO Cyber M&S federate internally consists of one user application, the EPVD and one service running without user interaction, the HLA WebLVC Server. The EPVD is a HLA NETN compliant web-based simulation control component that enables the user to initialize a simulation using MSDL or C2SIM LOX, view the current task organization, submit tasks to simulated entities, monitor progress, and view reports. It is a 'white cell' application and displays the ground truth of the simulation.

The EPVD has two views relevant for this experiment: the *Map view* and the *Cyber view*. The *Map view* shows `PhysicalEntities` on a topographical map. The *Cyber view* renders all the cyber objects as nodes and their relations as lines linking the nodes. Relations can, for example, indicate that one object 'provides' another object, or that one object is 'administered by' another object. Cyber interactions that affect objects or their relations will cause the nodes or links to be rendered in different styles.

Hadean Pattern-of-Life Simulation

Hadean provides a rich and detailed simulation background of the real world giving context and realism for training, planning, and mission rehearsal. Hadean simulates a realistic, highly detailed, and large-scale pattern-of-life, in a single environment, including a civilian population, civilian air and maritime traffic, social media, telecoms, satellites, and civil infrastructure. Hadean integrates with other capabilities using Distributed Interactive Simulation (DIS) and HLA standards.

Scenario

In this artificial scenario, we simulate humans holding a cellphone that is connected to one of the many telecom base stations situated inside a city. Cyberattacks are introduced that affect connectivity between phones and base stations. All humans and cyber devices are simulated by the Pattern-of-life simulation and visualized on the *Map* and *Cyber* views of the EPVD. The cyber effects and attacks are initiated from the EPVD application, affecting cyber objects inside the Pattern-of-Life simulation and possibly affecting the behavior of humans. The EPVD can introduce both cyberattacks and cyber effects. That is, the Cyber FOM makes a distinction between the attack and the effects that result from a (partly) successful attack. In this scenario, we introduce effects without simulating the attack, and introduce actual attacks that result in a certain effect.

CWIX Experiment

Tests with the federated simulation described in this section were performed at CWIX 2025. First, basic tests verifying connectivity and the communication of objects were performed. During these tests, both physical objects (described as RPR `PhysicalEntity` objects) and cyber objects (described as Cyber FOM `Device` and `NetworkLink` objects) were exchanged. Then, the capacity of the tooling was tested by sending approximately 200 entities and observing responsiveness of UI tools. Each entity continuously updates its locations and other variables with a one second interval. The third test focusses on cyber interactions and responses to those interactions. We injected a cyberattack using the EPVD by sending a `BlockTrafficEffect` to specific entities. This `BlockTrafficEffect` was expected to change the `Bandwidth` property of the `NetworkLink` to zero. The expected response was a visual change within the *Cyber view* interface of the EPVD: compromised connections are highlighted in red replacing the default green color. This visual feedback provides a representation of a disrupted connection in the simulation. Finally, a `CyberAttack` was injected using the EPVD with a `MitreSubtechniqueID` of 1499, i.e., an endpoint denial of service attack. The effect of this attack was expected to be identical to the `BlockTrafficEffect`. The Result section reports on testing outcomes.

CWIX Experiment results

This section present a concise overview of all results obtained at CWIX 2025 for the Federated Cyber Modeling and Simulation tests. Table 1 summarizes the outcomes of the first test, which consists of four subtest. The test focused on the initial connection to the RTI and the creation of a single `Device`, `NetworkLink` and `PhysicalEntity`. Each subtest was executed successfully, confirming the expected result as seen in the description column.

Sub	Description	Result	Succes
1	Connect to federation	Connected with aligned FOM files	Yes
2	Creation of `Device`	`Device` sent and received	Yes
3	Creation of the `NetworkLink`	`NetworkLink` sent and received	Yes
4	Creation of `PhysicalEntity`	`PhysicalEntity` sent and received	Yes

Table 1: Test 1: static entities

Table 2 summarizes the outcomes of the second test, which consists of three subtest. As a follow-up of test one we tested the creation of multiple `Devices`, `NetworkLinks` and `PhysicalEntities`. Whereas the `NetworkLinks` functioned as a connection between multiple `devices`. Each subtest was executed successfully, confirming the expected result as seen in the description.

Sub	Description	Result	Succes
1	Creation of `Devices`	Devices sent and received	Yes
2	Creation of the cyber `NetworkLinks`	`NetworkLinks` sent and received	Yes
3	Creation of `PhysicalEntities`	`PhysicalEntities` sent and received	Yes

Table 2: Test 2 Dynamic entities

Table 3 summarizes the outcomes of the third test, which consists of two subtest. As a follow-up of tests one and two the `BlockTrafficEffect` interaction on a `NetworkLink` was tested. Each subtest was executed successfully, confirming the expected result as seen in the description.

Sub	Description	Result	Succes
1	Send `BlockTrafficEffect` to a cyber `NetworkLink` of choice.	The `NetworkLink` connections are shown in red in the *Cyber view* (Figure 2).	Yes
2	Stop the `BlockTrafficEffect` by sending with phase “End”.	Connection with the `NetworkLink` is restored. Bandwidth > 0.0.	Yes

Table 3: Test 3 Cyber attacks

The final state of the EPVD shows the results of all three tests in Figure 2. The *Cyber view* as seen on the left shows `NetworkLinks` (pink) linked to `devices` (blue) as nodes. On the right the *Map view* can be seen with `PhysicalEntities` positioned based on their latitude and longitude. Whereas the `BlockTrafficEffect` from test three can be seen in the *Cyber view* by looking at the arrows shown in red (replacing the default green color) representing the blocked connection of `NetworkLinks`.

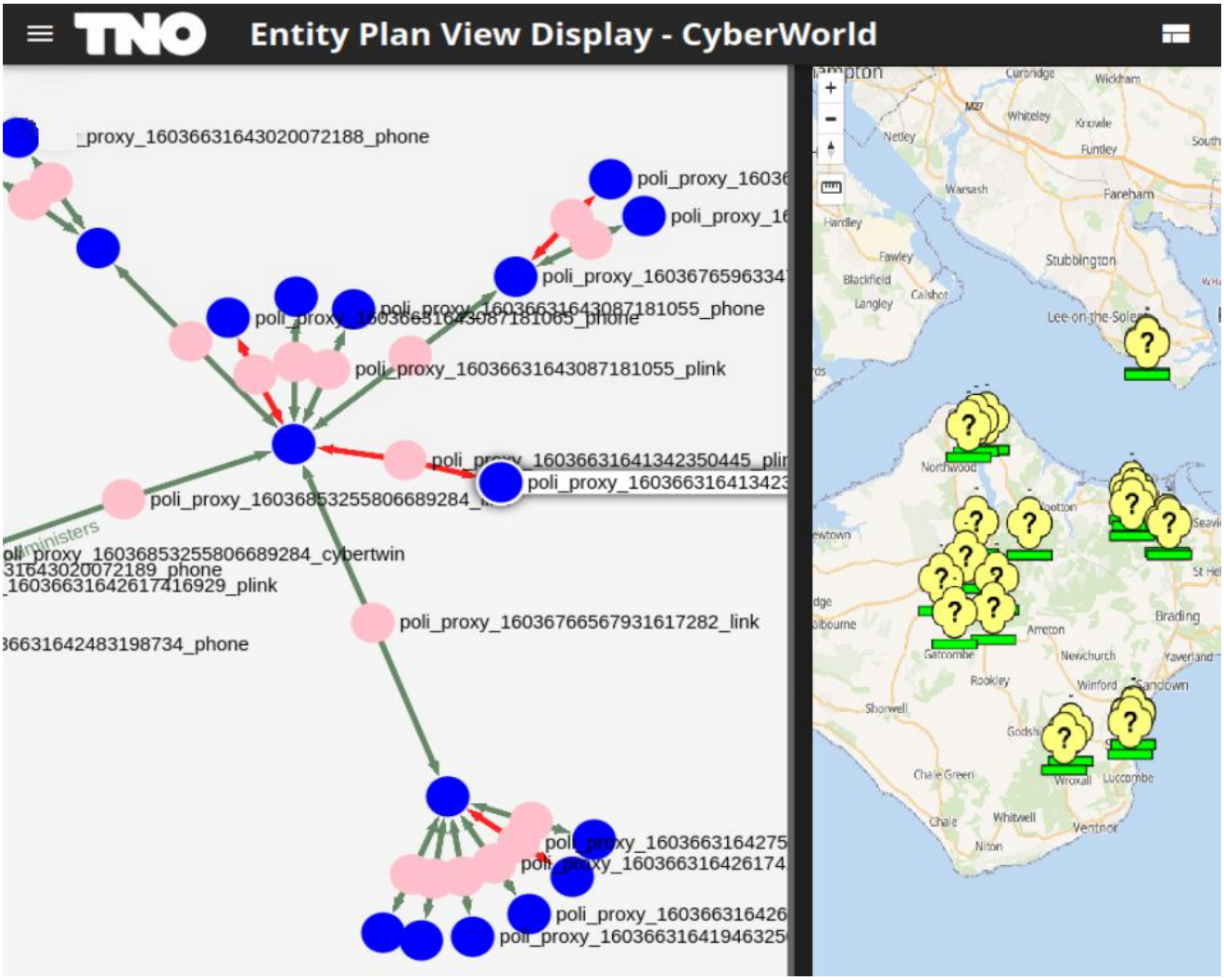

Figure 2: EPVD Cyber view and Map view after a `BlockTrafficEffect` was sent.

CONNECTING CYBER RANGES TO CYBER M&S

Connecting LVC simulations with cyber ranges could improve the fidelity of cyber entities and events in the simulation, and enhance training value for cyber range participants by increasing the complexity and interactivity of the scenario within which their activities take place. Although desirable, integrating an LVC simulation with a cyber range is not trivial given the very large number of elements (computers, operating systems, services, applications, APIs, storage devices, etc.) and events (wide variety of attacks, defensive actions, user responses, etc.) that can be present in a cyber range that *might* all need to be interfaced to the LVC simulation.

One might seek to avoid this problem by greatly limiting the 'allowable' actions a cyber warrior might take in the cyber range, and build just a couple of interfaces to the LVC simulation that are capable only of relaying the allowed actions. This would, however, greatly constraint the possible actions and so reduce the fidelity and training value for

the participants. Which might limit Cyber M&S and Cyber DEM adoption in the long term, especially given the need for cyber interfaces that can interpret and transmit all cyber effects across simulation domains (Bryan, et al (2019).

Although bidirectional communication between a cyber range and LVC simulation is desirable, we decided to scope our work and focus on communication from cyber range to LVC Simulation only.

Architecture

Broadly speaking, for the integration of a cyber range with an LVC simulation we can distinguish two architectural patterns. The first option consist of integration between individual components (systems, hardware, software, services, etc.), residing *within* the cyber range and the LVC simulation. That is, some or all components that are part of the cyber range would be equipped with an "LVC interface". We call this option the "bottom up" approach. The second option consists of integration with a central element in the cyber range, assuming the cyber range has one, that, by design, has the function to gather and hold information about all cyber entities, events and effects that are present in the cyber range. Such a central element could, for example, be a MISP instance to which defensive cyber entities report their observations. Note that a MISP instance operating in NATO context might only or additionally hold APP-11 messages containing similar information as is normally described by MISP-specific data structures. We therefore lump these two technologies together in this discussion.

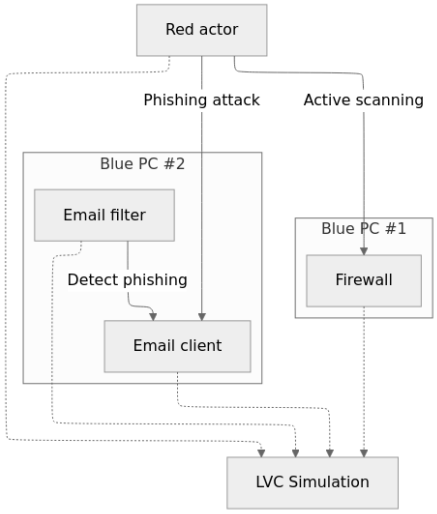

Figure 3: Example bottom up approach

The bottom up approach is illustrated in Figure 3 using an example. Consider a cyber range with virtual machines that mimic the personal computers of two employees working for a bank ("Blue #1" and "#2") and an adversary cyber attacker ("Red actor"). In this scenario, the cyber attacker is going to perform email phishing attacks by sending actual emails and perform an active scanning reconnaissance technique to find weaknesses in the firewalls. Those attacks should be communicated to the LVC simulation using the appropriate message types from the Cyber FOM. When integrating the cyber range with the LVC simulation at the application level, one would be required to build and maintain an interface between all the involved applications. Those applications might be closed source or otherwise hamper integrations with M&S specific libraries.

The top down approach is illustrated in Figure 4 for the same example. Here, the various applications do not have a direct interface with the simulation, but have an interface with MISP. For example, some email filter services or clients might have a MISP integration to receive and report up-to-date information on phishing attacks. The information stored in MISP is then mediated to the LVC simulation.

Advantages of the 'bottom up' architecture are: it is simple and straightforward to build for very specific effects, because there are fewer 'layers' between the actual application or effect and the connection to the LVC simulation. Disadvantages include that a specific interface should be built for each application and so it does not scale for more complex cyber ranges. Furthermore, those interfaces will probably need some 'intelligence' to detect the intent of a human actor, whereas a cyber attacker tries to hide. Also, many applications are closed-source so they cannot easily be extended with a highly specific M&S interface. Finally, cyber events and effects may be distributed over many entities (e.g., a DDoS attack launched from many computers), such that it is not clear where the 'connector' should be placed.

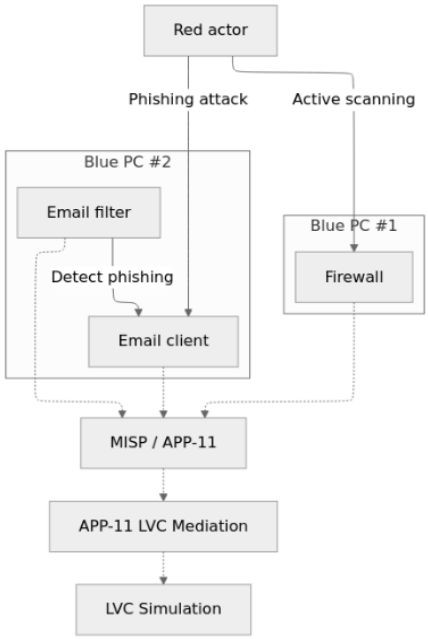

Figure 4: Example top down approach

Advantages of the 'top down' architecture are that a lot of integration work (i.e., the work to integrate an application with MISP) can be reused and comes 'for free'. That is, you 'only' need to build one mediation service between MISP and the LVC simulation. A major and obvious disadvantage of this approach is that this solution only works for things that have a functional MISP interface. Also, only objects and interactions that are detected by something reporting to MISP will reach the LVC simulation. As such, this method will not be able to communicate the "ground truth" to the LVC simulation. Finally, this architecture is only an option for the direction cyber range to LVC simulation, not the other way around.

At this stage of our research it is not possible to conclude what architectural pattern would be 'best'. It is likely that practical solutions can hold elements of both. However, given the potential advantages of the 'top down' option – specifically, the universality of the solution – we decide to explore this option in more detail, by implementing a mediation service between APP-11 Cyber messages residing in MISP and the Cyber FOM, where the term *mediation service* is typically used to indicate an application that translates ("mediates") communication between a non-M&S component and the simulation.

Mediation between APP-11 and Cyber FOM

To establish a first baseline for our mediation tests the following entities are mediated; `PhysicalEntity`, `device` and `application`. The `PhysicalEntity` contains geographical information, whereas the device and application entities are Cyber FOM objects which contain relevant cyber information. Information like IP addresses and software names, software versions. An example of the mapping of those FOM objects with the APP-11 reports can be found in Figure 5. In the upper right we find the APP-11 information example with colored variables. Variables which can be mapped either to the Cyber FOM or RPR FOM or to both. These elements play a crucial role in identifying vulnerabilities and are relevant in most cyber defense scenarios, particularly for threat detection and responses. While mediating APP-11 messages the change over time is visible in the output both on a geographical level and in the cyber layer. The final output of the mediation is an overview of all entities in their final state based on the APP-11 messages sent during set of cyber events.

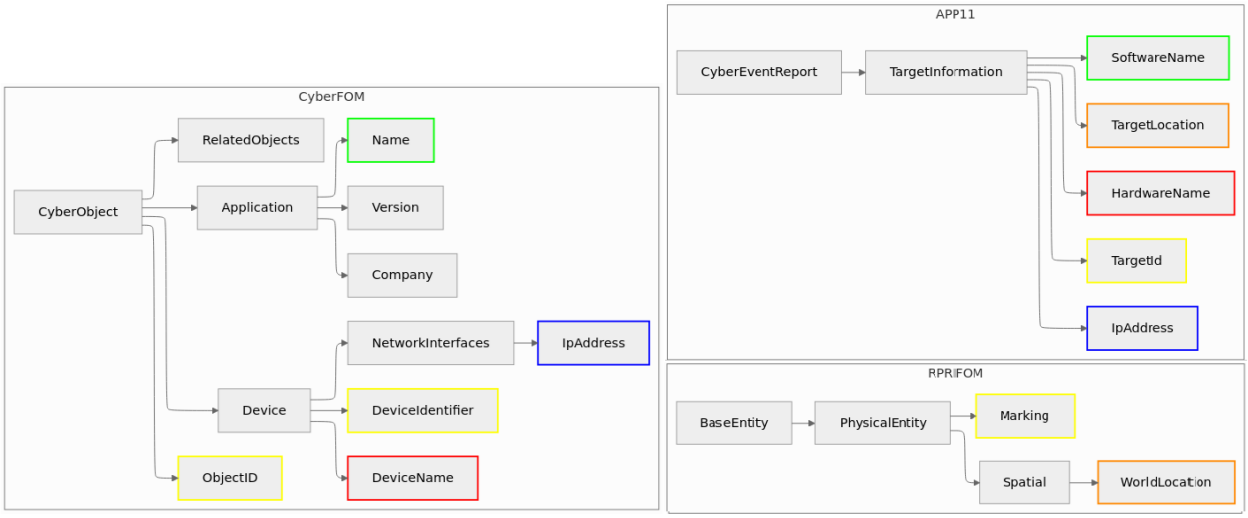

Figure 5: RPR FOM and Cyber FOM object mapping with APP-11

CWIX Exploration

During CWIX 2025, we explored the technical feasibility of our mediation service by connecting with capabilities that deployed a MISP platform containing APP-11 CMS messages. We then attempted to interpret the information stored inside those messages by observing a visualization of the mediated Cyber FOM messages. That interpretation was then checked with the team from which the messages originated. As such, few predetermined tests were performed. The added value of performing this explorative work at CWIX was that the APP-11 Cyber messages to be mediated were different, more extensive, and more realistic than the set of example messages available during development.

CWIX Exploration results

This section present a concise overview of all results obtained at CWIX 2025 for the mediation between APP-11 and the Cyber FOM. Using MISP we received four reports containing cyber event information. We processed these MISP messages and extracted the APP-11 information. Using this APP-11 data we successfully extracted three different types; `PhysicalEntity`, `Device` and `Application` for all four reports received. The relations between these entities could also be determined and was added to the created entities. After extraction we used the WebLVC server to send the retrieved entities to the RTI. The extracted information was then used to construct a high level overview both in the *Cyber view* and *Map view* of the EPVD.

DISCUSSION

Our main observation from the work done within the scope of this paper is that the Cyber FOM effectively facilitated all the desired data exchanges. That is, we did not encounter cyber objects or interactions that could not be represented using one of the available types in the Cyber DEM. Also, all object properties that were relevant for these tests could be transmitted using one of the properties defined in the Cyber DEM. Admittedly, the level of detail exchanged between the two simulators was not very deep: our tests did not 'challenge' the Cyber DEM extensively. Nevertheless, we do believe that this particular setup was a more elaborate test of the Cyber DEM than any prior simulations that were reported on by other authors (NMSG-200, in preparation).

During the development of the simulation, some discussion arose about how to properly model networks and `NetworkLinks` between `devices`. That is, one possible understanding is that the `RelatedObjects` field of a `CyberObject` should be used to describe the 'connectedness' of two objects, and so the use of `NetworkLink` objects is optional. The understanding we settled on is that a `NetworkLink` object should be created to connect the two objects. We recommend to add minor clarifications in the Cyber DEM documentation.

A limitation of the current version of the Cyber DEM relates to the modeling of large networks with many connected devices, or networks that should not be modelled in great detail. Technically, all `Device` objects that are part of a network should have a `NetworkLink` to all other Device objects in the network, resulting in a very large number of links. This approach requires the full specification of the network topology (i.e., routers, switches, etc.). There are possibly also use cases where it is sufficient to model a Device to be connected to a Network, but this is currently unsupported, as only `Device` and `NetworkLink` object types have a `NetworkInterfaces` property. Future iterations of the standard could include more abstract and flexible representations of the network implementation. Ongoing work, including our own, can help inform and support these developments within the Cyber DEM product development group.

We feel that the presented simulation could already be of great value for enriching existing training simulations with certain cyber effects. The Pattern-of-Life simulation provides a rich additional layer to a simulation, featuring both 'human' and 'cyber' elements. Our tests show that the Pattern-of-Life simulation can be controlled effectively by a third party white cell application, such as the EPVD considered here.

Previous simulations involving cyber built by the authors of this paper typically did not feature more than a handful of cyber entities. During some of our tests at CWIX, more than 200 cyber entities were present in the simulation. Based on this experience, we feel that the *Cyber view* of the EPVD application is a very useful tool for a white cell application for cyber simulation. The 'network perspective' seems to map easily with our mental model of cyberspace and we were able to quickly find objects. Drawing the same information on top of a geographic map (the *Map view*) would needlessly clutter the view.

On the topic of the integration of cyber ranges with LVC simulation, our observations and conclusions are less concrete. The work described in this paper was our first encounter with the topic and few publications, if any, provided us with a useful starting point. Our exploration with a MISP and APP-11 mediation service (following the 'top down' architecture) was largely driven by the believe that the alternative (the 'bottom up' architecture) would introduce a lot of complexity, require a large development effort, and is not possible for systems and applications that are not open for modification. The initial experiments with APP-11 were successful, but also indicated that it cannot be a solution for the short-term, given its relative novelty. Future work should investigate whether the information typically shared

within MISP itself could be a viable alternative source for mediation. We also believe that the 'bottom up' approach should be investigated properly.

CONCLUSION / RECOMMENDATIONS

From the work presented in this paper, we conclude that the SISO Cyber DEM is an effective tool for data exchange within a federated simulation environment. No major shortcomings were identified, although some confusion remains on how certain network topologies are supposed to be modelled, which should be investigated further. Concerning the integration of cyber ranges with LVC simulation, we see our work as a first exploratory step and believe that more concrete, operationally relevant use-cases provided by the appropriate stakeholders should guide our next steps.

ACKNOWLEDGEMENTS

We are thankful for the constructive collaboration and fruitful discussions with our CWIX testing partners, in particular Hadean Supercomputing and the APP-11 Cyber Message Standard capabilities.

REFERENCES

Bryan, D., Wells, D., Morse, K. L., Hofstra, K., Meyer, S., & Ruth, J. (2019). *A Roadmap to Achieve Cyber Modeling & Simulation Interoperability. Training, Simulation and Education Conference (I/ITSEC).* Paper ID 19314. www.xcdsystem.com/iitsec/19314_0823033116.pdf

Dahmann, J. S., Fujimoto, R. M., & Weatherly, R. M. (1997, December). The department of defense high level architecture. In *Proceedings of the 29th conference on Winter simulation* (pp. 142-149).

Delvecchio, P., Galantucci, S., Iannacone, A. et al. (2025). CARIOCA: prioritizing the use of IoC by threats assessment shared on the MISP platform. Int. J. Inf. Secur. 24, 98. https://doi.org/10.1007/s10207-025-01006-2
IEEE. (2010). *IEEE standard for modeling and simulation (M&S) high level architecture (HLA) – Framework and rules* (IEEE Std 1516-2010). IEEE. IEEE SA - IEEE 1516-2010

MISP Project. (2016). *MISP threat intelligence platform*. MISP Project https://www.misp-project.org

NATO Modeling and Simulation Group (NMSG). (2020). *NATO Education and Training Network Federation Object Model (NETN FOM)*. AMSP-04. AMSP-04 NETN FAFD | NATO Simulation Standards

NATO Standardization Office. (n.d.). *Cyber Security Information Sharing – AdatP-5660 Edition A* (STANAG No. 5660). NATO

NATO Standardization Office. (2024). *NATO Message Catalogue* (STANAG No. 7149). NATO

NMSG-200 (not yet published, expected 2025) *MSG-ST-200 Final Report.* Modeling and Simulation Group 200

Ramsdale, A., Shiaeles, S., & Kolokotronis, N. (2020). A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages. *Electronics*, *9*(5), 824. https://doi.org/10.3390/electronics9050824

SISO. (2015). *Standard for real-time platform reference federation object model (RPR FOM)*, version 2.0 (SISO-STD-001-2015). Simulation Interoperability Standards Organization. siso-std-001-2015_grim_rpr_f.pdf

SISO. (2022). *Standard for Web Live, Virtual, Constructive (WebLVC) Protocol* (SISO-STD-017-2022). Simulation Interoperability Standards Organization. siso-std-017-2022_weblvc_pro.pdf

SISO. (2023). *Standard for cyber data exchange model (Cyber DEM)* (SISO-STD-025-2023). Simulation Interoperability Standards Organization. siso-std-025-2023_cyberdem.pdf

SISO. (2024). *Standard for Cyber Federation Object Model (Cyber FOM)* (SISO-STD-025.3-2024). Simulation Interoperability Standards Organization. siso-std-025.3-2024.xml

Smith, M. (2024). *Fortifying the Virtual Battlefield: Integrating Cyber Effects using Simulation*. *Training, Simulation and Education Conference (I/ITSEC)*. Paper ID 24208.
www.xcdsystem.com/iitsec/24208_0828055530.3.pdf