SISO
Simulation Interoperability
Standards Organization
"Simulation Interoperability & Reuse through Standards"

SISO-REF-072-2024

Reference for Cyber Data Exchange Model (DEM) Base Objects, Networks, Effects, & Specifications (BONES)

25 January 2024

SAC Approved: 02/21/2024 **EXCOM Approved: 03/27/2024**

Prepared by:
Cyber Data Exchange Model (DEM) Product Development Group

Please note that this document may be revised periodically. The latest edition will be made available at the SISO website at no charge. The document on the SISO website is considered to be the definitive version.

SISO Inc. Board of Directors
7901 4th St. N, Suite 300-4043
St. Petersburg, FL 33702, USA

Revision History

Version	Section	Date (MM/DD/YYY)	Description
1.0	All	11/30/2019	Initial version
Draft 1	All	3/31/2022	Draft at the end of comment round 1
Draft 2	All	11/14/2022	Draft at the end of comment round 2
Draft 3	1.5.2, 2.2, 5, 6, 6.1, 6.1.2.1, 6.1.4, 6.1.5, 6.1.5.1, 6.1.5.2, 6.2, 6.2.2.2, 6.2.2.2.3, 6.2.2.3, 6.2.2.4, 6.2.3.1.1.2, 6.2.3.1.1.5, 6.2.3.3, 6.4, 7.3, 8.1	1/10/2024	Updated based on comment adjudication for the Cyber DEM ballot and PDG membership
Final	Tables of Contents and Lists of Figures and Tables	1/25/2024	Final edits for publication

Table of Contents

List of Figures

List of Tables

1 INTRODUCTION

The Cyber Data Exchange Model (DEM) represents cyber events and objects in a format independent of simulation interoperability solutions, but which is unambiguously translatable to those solutions. The Cyber DEM provides the common representation of these cyberspace conditions so they can be transmitted bi-directionally between cyber ranges, cyber simulations, and the Live-Virtual-Constructive (LVC) environments supported by traditional kinetic simulation.

1.1 Purpose

This document describes the structure and use of the Cyber DEM.

1.2 Scope

There is limited capability to incorporate realistic cyber events, attacks, effects, and responses into LVC environments because traditional kinetic simulations and cyber ranges are not well integrated. The lack of integration limits the incorporation of realistic cyberspace conditions, created within cyber ranges, into the operational systems and simulations that form the test environment or training environment. As a result, systems under test cannot be tested under the conditions in which they will operate, nor are warfighters able to be trained under the conditions in which they will fight.

The lack of integration can be overcome through a mechanism that provides a common syntax and semantics for transferring information between kinetic environments and cyber ranges and satisfies information assurance requirements. The Cyber DEM provides the common representation of these cyberspace conditions so they can be transmitted bi-directionally between cyber ranges and the test / training environments supported by traditional kinetic simulation.

1.3 Objectives

The Cyber DEM seeks to represent cyber events and objects in a format independent of simulation interoperability solutions, but which is unambiguously translatable to those solutions (see section 6.2.1). In this way it is somewhat analogous to SISO's Real-time Platform Reference Federation Object Model (RPR FOM). These cyber events and objects are designed to support the broadest range of use cases known at its time of development across all communities supported by simulation. It is also intended to support use cases foreseeable in the near future.

1.4 Intended Audience

Potential Cyber DEM users are the intended audience for this document.

1.5 Acknowledgments

1.5.1 Participants

At the time this product was submitted to the Standards Activity Committee (SAC) for approval, the Cyber DEM PDG had the following membership and was assigned the following SAC Technical Area Director:

1.5.2 Product Development Group

Dr. Katherine L. Morse (Chair)

Dr. Ed Powell (Vice-Chair)

Dr. Fuzzy Wells (Secretary)

Clyde Smithson (SAC Technical Area Director)

Grant Bailey

Paolo Barthelmess

Dr. Curtis Blais

Dr. Bert Boltjes

Edward Bowen

Jordan Dauble

Tim Friest

Allen Geddes

Cristian Gheorghiu

Rotem Guttman

Dr. Omar Hasan

Björn Löfstrand

Farid Mamaghani

Matthew McGlawn

Christopher Metevier

Sara Meyer

Dawn Moffat

Ivar Oswalt

David Ronnfeldt

Heath Rush

John Rutledge

Kevin Seavey

Graham Shanks

Jason Strauss

John Tapsfield

Tom van den Berg

René Verhage

Jeffrey Welch

Kevin Wood

2 REFERENCES

2.1 SISO Documents

The following SISO documents were used in generating this document. When the following documents are superseded by an approved revision and that causes a conflict with this document, the revision of the below-referenced documents shall supersede this document. These documents are available through the SISO web site at https://sisostandards.connectedcommunity.org/communities/community-home/librarydocuments?communitykey=d888b620-620e-445d-81bf-f10a3aa1c3af&LibraryFolderKey=&DefaultView=&defaultview=folder.

Document Number	Title
SISO-REF-070-2019	Final Report for the Cyber Modeling and Simulation (M&S) Study Group (SG)

Document Number	Title
SISO-REF-072-2020	Cyber Data Exchange Model (DEM) reference product
SISO-PN-025-2020	Cyber DEM Product Nomination
SISO-STD-001.1-2015	Standard for Real-time Platform Reference Federation Object Model (RPR FOM)
SISO-REF-010-2023	Reference for Enumerations for Simulation Interoperability, Version 31
SISO-STD-025-2023, SISO-STD-025-2023.1, SISO-STD-025-2023.2	Cyber Data Exchange Model (DEM)
SISO-STD-025.1-Draft	Cyber DEM Objects
SISO-STD-025.2-Draft	Cyber DEM Events
SISO Product Data File	Code Archives: COBWebS High Level Architecture (HLA) Code Example, Test & Training Enabling Architecture (TENA) Retina Code Example, JSON Schema[1]
SISO Product Data File	UMLet UXF Parser[2]

2.2 Other Documents

Document Number	Title
N/A	"The DoD Cyber Strategy," April 2015, https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf
JP 3-12	"Cyberspace Operations," https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf
IEEE Std 1516™-2010, IEEE Std 1516™-2010.1, IEEE Std 1516™-2010-2	Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)
IEEE 1278.1-2012	IEEE Standard for Distributed Interactive Simulation (DIS) – Application Protocols
ATT&CK v13	MITRE, "Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework," v13, 25 April 2023, https://attack.mitre.org/
Lexico	Definitions of action and effect, www.lexico.com
Techopedia	Definition of data exfiltration, www.techopedia.com
FM 3-12	US Army, "FM 3-12 Cyberspace Operations and Electromagnetic Warfare," August 2021, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN33127-FM_3-12-000-WEB-1.pdf

[1] https://sisostandards.connectedcommunity.org/viewdocument/code-archives?CommunityKey=d888b620-620e-445d-81bf-f10a3aa1c3af&tab=librarydocuments&LibraryFolderKey=92242a29-da9a-496f-87a2-0188c7c960b4&DefaultView=folder

[2] https://sisostandards.connectedcommunity.org/viewdocument/uxf-parser?CommunityKey=d888b620-620e-445d-81bf-f10a3aa1c3af&tab=librarydocuments&LibraryFolderKey=9e95adf1-0265-4df2-9a2b-0188f9e96294&DefaultView=folder

Document Number	Title
MITRE MTR13-4173	Deborah J. Bodeau and Richard D. Graubart, “Characterizing Effects on the Cyber Adversary,” November 2013, https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf
Rumbaugh, Jacobson, and Booch	James Rumbaugh, Ivar Jacobson, and Grady Booch (2005). The Unified Modeling Language Reference Manual, Second Edition. Addison-Wesley:Upper Saddle River NJ.
D3FEND	MITRE, “Detection, Denial, and Disruption Framework Empowering Network Defense”, 0.12.0-BETA-2, 21 Mar 2023, https://d3fend.mitre.org/

3 DEFINITIONS

Cardinality — The number of elements in a set. It is a specific number. Contrast with multiplicity, which is a range of possible cardinalities a set may hold. [Rumbaugh, Jacobson, and Booch]

Cyber event — Cyber Events represent non-persistent cyber actions and effects as opposed to persistent cyber objects

Cyber object — A Cyber Object is an entity in cyberspace (physical, logical, or persona layers)

Multiplicity — A specification of the range of allowable cardinality values—the sizes—that a collection may assume. Multiplicity specifications may be given for association ends, attributes, parts within composite classes, repetitions of messages, and other purposes. In principle, a multiplicity is a (possibly infinite) subset of the non-negative integers. In practice, it is an integer interval. If multiplicity is greater than one, it includes an indication of whether the elements are ordered and unique. [Rumbaugh, Jacobson, and Booch]

4 ACRONYMS AND ABBREVIATIONS

Acronym/Abbr	Definition
AMT	Architecture Management Team
COBWebS	Cyber Operations Battlefield Web Services
CyberBOSS	Cyberspace Battlefield Operating System Simulation
DEM	Data Exchange Model
DCO	Defensive Cyber Operations
DIS	Distributed Interactive Simulation
DoD	Department of Defense
ECMA	European Computer Manufacturer's Association
FOM	Federation Object Model
JBC-P	Joint Battle Command Platform
JSON	JavaScript Object Notation
HLA	High Level Architecture
M&S	Modeling and Simulation
DCO	Defensive Cyber Operations
PDU	Protocol Data Unit

Acronym/Abbr	Definition
RPR	Real-time Platform Reference FOM
SG	Study Group
SISO	Simulation Interoperability Standards Organization
SWG	Special Working Group
tdl	TENA Definition Language
TDL	Tactical Data Link
TENA	Test and Training Enabling Architecture
ToR	Terms of Reference
UML	Unified Modeling Language
VMF	Variable Message Format
XML	Extensible Markup Language

5 Design Patterns

Several design patterns were identified and implemented over the course of the draft Cyber DEM development:

1. *Follow design patterns already widely used in kinetic simulations*. For example, in a kinetic engagement, reconnaissance is typically NOT modeled through simple object discovery which represents ground truth. Calculations based on that ground truth are made to determine the success of reconnaissance. We have replicated that pattern in the Cyber DEM through Cyber Event/Cyber Action/Cyber Recon.
2. *Assume inheritance of datatypes from existing data models,* e.g. time. There are many representations used in kinetic simulations. Their use is the subject of federation agreements. Rather than trying to import an exhaustive list of those into the Cyber DEM, it is assumed that the time representation used in any associated kinetic simulation will be used in the cyber simulation as well. In cases where there is no associated kinetic simulation, a federation agreement can be made for a time representation appropriate for a cyber-only simulation.
3. *Cyber events can't target non-cyber objects.* The non-cyber objects must have a cyber element or associated cyber object that is the target, e.g. a C2 system on a ground platform or a processor on a drone.
4. *Provide a solid structure while allowing for future extensions.* Because cyber M&S is still nascent, the use cases are currently limited to fairly broad effects. More detailed, nuanced attacks and effects will obviously be required in the future. Where the Cyber DEM PDG recognized the challenge of developing detailed parameterizations of such attacks at this time, e.g. Manipulation Attack, we have inserted a class in the model and specified a data blob as the content. Such classes should be decomposed and standardized in the future when implementation experience identifies useful structures.
5. *Provide hooks for associated tools, e.g. data and event logging and visualization.* Two tools adding prototype Cyber DEM capability are TENA Retina and the TENA Data Collection System (TDCS).
    a. TENA Retina is a visualization tool focused on providing cyber white cell teams visibility into cyber actions and the cyber environment during a test or training event. TENA Retina aggregates updates on cyber objects and observations into displays to provide situational awareness for white cell team members. TENA Retina will be delivered with a TENA implementation of the DRAFT Cyber DEM object model.

   b. TDCS is a data collection and playback mechanism for TENA object models. The data collectors are automatically generated from TENA definition files and are available in the TENA Repository. A TDCS data collector and playback tool is available for the DRAFT Cyber DEM object model in the TENA Repository. See Section 8.3 “Test & Training Enabling Architecture (TENA)” for details on downloading the TDCS data collector.

6. *MITRE ATT&CK™ & D3FEND™[ATT&CK v13, D3FEND] information should be secondary to primary representation in the rest of the Cyber DEM.* MITRE ATT&CK and D3FEND framework representation is included for completeness, but a significant portion of that framework can be represented in the rest of the Cyber DEM. Preference should be given to the rest of the Cyber DEM as the primary representation because more complete information is allowed.

6 Structure of the Cyber DEM

As previously mentioned, the Cyber DEM represents Cyber Objects and Events. Cyber Objects are persistent just like objects in the High Level Architecture (HLA) and the Test & Training Enabling Architecture (TENA). In DIS, cyber objects will provide additional information for simulation entities and will be sent at heartbeat intervals similar to Entity State PDUs to indicate persistence. Cyber Events are slightly different than kinetic events in that they can persist over time. The mechanism for their persistence is described in section 0. The Cyber DEM uses persistent and message stereotypes for the root node of the object and event class hierarchies, respectively, to enable automatic code generation where appropriate, especially for TENA. Both Cyber Objects and Cyber Events are supported by additional data structures.

The Cyber DEM PDG chose Unified Modeling Language (UML) as the architecture-neutral representation, primarily because of the value of visualization to understanding and organizing the Cyber DEM. The team chose the open source UML editor UMLet (https://www.umlet.com/). The Cyber DEM reference product, SISO-REF-072-2020, uses this tool’s format, Unified Modeling Language (UML) Exchange Format (UXF), which is an Extensible Markup Language (XML) schema.

Enumerations are used in both branches of the Cyber DEM. Where the Enumerations for Simulation Interoperability [SISO-REF-010-2018] are applicable, they have been reused and / or extensions proposed, e.g. Data Link Protocol Type proposes extensions for Tactical Data Links (TDL) [UID 178]. All extended and new enumerations have been proposed to the Enumerations Special Working Group (SWG) for inclusion in SISO-REF-010.

If a simulation requires additions to enumerations, the developers should use the common practice of extending enumerations locally and sharing these extensions with the Enumerations SWG for inclusion in future versions of SISO-REF-010.

In UML diagrams, the multiplicity of an attribute is expressed in the form datatype[min..max], where the default number is assumed to be [1..1] similarly to XML, min=1 and max=1 if not specified.

The Cyber DEM naming convention uses Pascal case.

6.1 Objects

A Cyber Object is an entity in cyberspace (physical, logical, or persona layers).

All Cyber Objects have an ID to support targeting and a Name string to support visualization and analysis.

Table 1: Cyber Object

Attribute	Multiplicity	Description
ObjectID		A federation unique identifier for the object
Name	[0..1]	String identifier for use in user interfaces, visualization, analysis, etc.
Description	[0..1]	A short description of the object

Attribute	Multiplicity	Description
RelatedObjects	[*]	The type of relationship identified between this object and other objects, such as Administer, AdministeredBy, ComponentOf, HasComponent

Pursuant to design pattern 4, Cyber Object also contains a description string. We foresee the need to identify cyber objects not already derived from Cyber Object. Such objects can be instantiated as “generic” Cyber Objects where the description string provides sufficient detail for the associated simulation to operate on it. Such derivations should also be submitted for future standardization to support the applicability and stability of the Cyber DEM going forward. The description also supports design pattern 5.

Cyber Object allows for identifying any number of related objects through its Related Objects array. This is to support the reality that cyber objects can be related in ways that are not physically obvious in the same way that kinetic objects are, e.g. as a result of geographic location. Cyber Object could relate to the physical entity through the Related Object Struct. A Cyber Object could also extend the physical entity to which it’s related.

As with all such flexible mechanisms, Related Objects also doesn’t prevent relationships that don’t make sense. For example, a persona can administrate a device, system, or network, but it doesn’t make sense for a persona to be a component of a device or for a device to administer a persona. Precluding such representations falls under the purview of federation agreements.

Figure 1 illustrates the Cyber DEM Objects model. All objects are derived from the top-level class, Cyber Object.

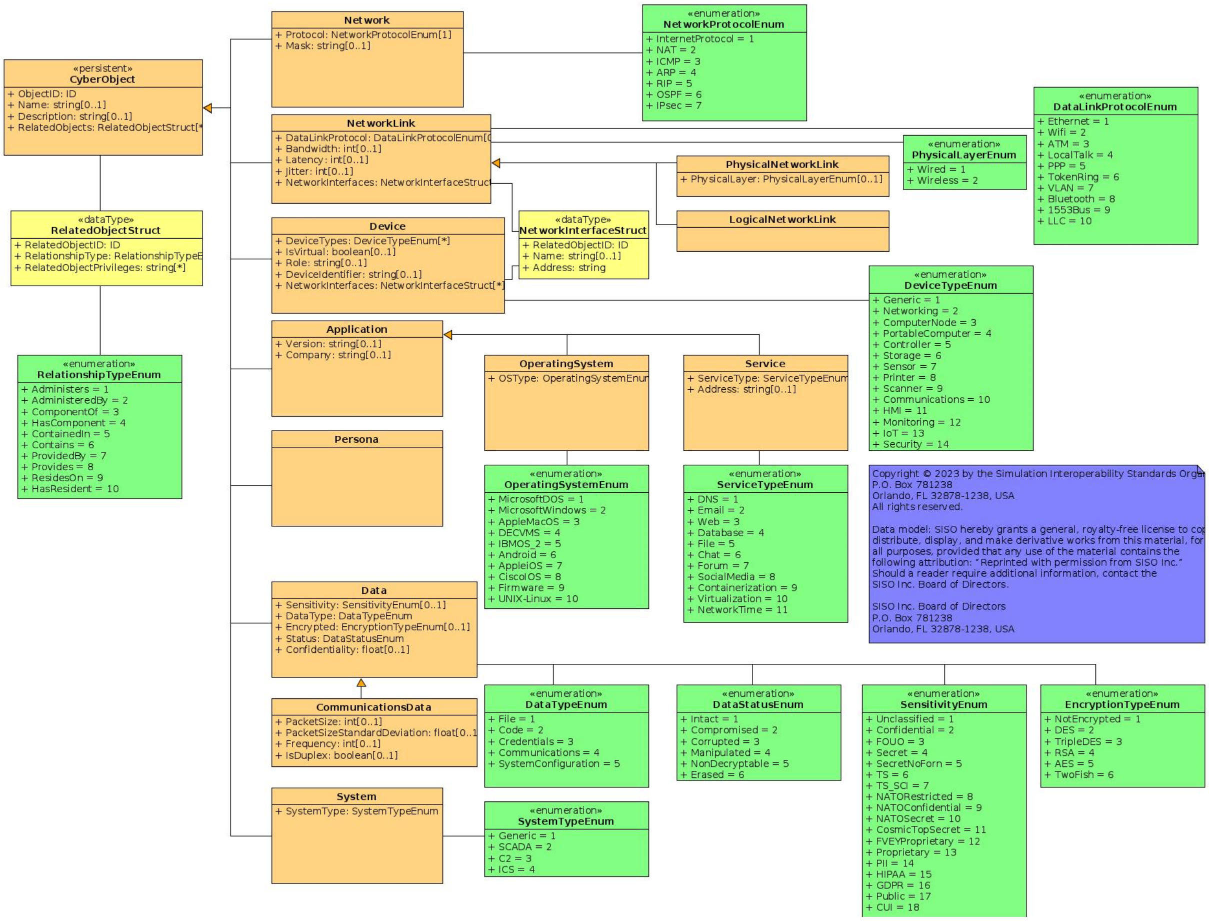

Figure 1: Cyber Objects Model

Each of the subclasses of Cyber Object is described in the following subsections.

6.1.1 Application

Application represents a specific instance of a software program running on a device. Running processes are considered to be members of this class. At rest applications are considered to be members of the Data class with Data Type Code.

Table 2: Application

Attribute	Multiplicity	Description
Version	[0..1]	Vendor or developer assigned version
Company	[0..1]	Developer/Producer name

6.1.1.1 Operating System

Operating System represents the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.

Table 3: Operating System

Attribute	Multiplicity	Description
OSType		Type of software supporting a computer's basic functions, such as UNIX-Linux, MicrosoftWindows, Android, AppleiOS, etc.

To associate 0 or more IP Addresses with an Operating System, multiple Cyber Objects can be created and relationships can be established with the Related Objects array.

6.1.1.2 Service

Service represents an application that provides a service to network clients.

Table 4: Service

Attribute	Multiplicity	Description
ServiceType		Type of service, such as DNS, Email, Web, Database, etc.
Address	[0..1]	A service defined address (e.g. web servers have URLs, database servers have connection strings, etc.)

6.1.2 Data

Data represents information encapsulated in an instance or collection of file(s), message(s), or record(s) in a database. Data can represent a specific information object or a kind of information, e.g. a specific tactical message or messages that contain SPOTREP information. CyberObject.Name is the filename, subject, information kind, etc. At rest applications are considered to be members of this class with Data Type Code. Running processes are considered to be members of the Application class.

Table 5: Data

Attribute	Multiplicity	Description
Sensitivity	[0..1]	Classification or distribution restrictions
DataType		Type of the data
Encrypted	[0..1]	Encryption type used on the data

Attribute	Multiplicity	Description
Status		Status/integrity of the data
Confidentiality	[0..1]	100% means complete confidentiality, 0% means total loss of confidentiality

6.1.2.1 Communications Data

Communications Data represents data on a communications channel/stream.

Table 6: Communications Data

Attribute	Multiplicity	Description
PacketSize	[0..1]	Average size (in bytes) of individual packets
PacketSizeStandardDeviation	[0..1]	Variability of packet sizes (0.0 for fixed sized packets)
Frequency	[0..1]	Packets per second
IsDuplex	[0..1]	True if the communications bidirectional

6.1.3 Device

Device represents an electronic device capable of operating in cyberspace.

Table 7: Device

Attribute	Multiplicity	Description
DeviceTypes	[*]	The kind of device (multi-purpose devices would have multiple types)
IsVirtual	[0..1]	Is the device virtualized (e.g. a VM)
Role	[0..1]	Describes the purpose of the devices that are part of a system or network (e.g. domain controller or system controller)
DeviceIdentifier	[0..1]	Device unique identifier, e.g. uniform resource number (URN)
NetworkInterfaces	[*]	The endpoints of the network link

6.1.4 Network

Network represents a data network including LANs, WANs, tactical radio data networks, cellular data networks, etc.; networks can be composed of other networks, e.g. a WAN is a collection of LANs. CyberObject.Name is the domain name or subnet address range.

Table 8: Network

Attribute	Multiplicity	Description
Protocol		The OSI Model network layer

Attribute	Multiplicity	Description
Mask	[0..1]	Used to divide networks into subnets: the format of the mask is dependent upon the networking protocol. IPv4 would use the quad-dotted decimal notation, e.g. 255.255.255.x.

6.1.5 Network Link

Network Link represents a physical or logical data link or bus between two or more devices.

Table 9: Network Link

Attribute	Multiplicity	Description
DataLinkProtocol	[0..1]	DataLinkProtocol specifies the protocol between network interfaces on this link
Bandwidth	[0..1]	Maximum throughput of the link (in bits/second)
Latency	[0..1]	Delay between sending and receiving of packets (in milliseconds)
Jitter	[0..1]	Duration between individual packets (in milliseconds)
NetworkInterfaces	[*]	The endpoints of the network link

6.1.5.1 Physical Network Link

Physical Network Link represents physical data link (or bus) between two or more devices.

Attribute	Multiplicity	Description
PhysicalLayer	[0..1]	The hardware means of sending and receiving data on a carrier (OSI Model layer 1)

6.1.5.2 Logical Network Link

Logical Network Link represents a logical data link (or bus) between two or more devices. Logical Network Link is an abstract class intended as an organizational construct.

6.1.6 Persona

Persona represents a user or profile for a person within cyberspace. CyberObject.Name is the username, email address, etc. Persona is currently a placeholder and organizational construct for identifying personae. It has no attributes.

6.1.7 System

System represents a collection of Cyber Objects, i.e. components and / or subsystems, that work together.

Table 10: System

Attribute	Multiplicity	Description
SystemType		Type of system, such as SCADA, C2, ICS, etc.

6.2 Events

Events represent non-persistent cyber actions and effects as opposed to persistent cyber objects. All events are derived from the top-level class, Cyber Event.

Table 11: Cyber Event

Attribute	Multiplicity	Description
EventID		Federation-unique ID for the event to support future actions, e.g. Suspend
Description	[0..1]	A human readable description of the event
EventTime		Simulation time of the current phase of the CyberEvent
TargetIDs	[*]	An array of object IDs representing targets
TargetModifiers	[*]	Key-value pairs providing additional filtering criteria for the target(s)
Phase		Execution phase of a Cyber Event, such as Start, Suspend, Resume, End, etc.
Duration		Length of time (in seconds) the event occurs
ActorIDs	[*]	A List of IDs of the perpetrators involved in this Cyber Event
SourceIDs	[0..*]	A list of IDs of the simulations that this Cyber Event came from
Payload	[0..1]	Contains the details of the event itself (including an indication if the details are inserted/updated/deleted) OR the message after the event, as decided by the federation agreement
RequestAcknowledgement		True if the receiver should send an acknowledgement back to the sender

Cyber Events can be long-lived in a manner unlike most kinetic events and effects, hence the Cyber Event Phase Type. An event can be suspended and continued. The continuation can include a modification, and an ongoing event can be modified. All Cyber Events have an ID to support this process. Setting Duration to 0 represents an instantaneous event. Indefinite / infinite duration events are represented with simulation interoperability solution specific representations, e.g. infinity in HLA or maximum value of a 16-bit integer in DIS.

Specification of targets is particularly challenging because they lack the convenient physical aspects of kinetic objects and actions such as detonations impacting geographic regions. Furthermore, cyber targets can have multiple aspects, e.g. a particular message type over a particular network. The array of Target Modifiers identifies these individual aspects. The presence of multiple Target Modifiers is understood to represent the intersection (logical and-ing) of these aspects, i.e. that all aspects must be true about an object for it to be a valid target. In the case where the target includes multiple instances of the same class of target, they can be represented in the array of Target IDs in the Cyber Event. Pursuant to design pattern 4, Target Modifier Key Value Pairs can be used to further describe detailed filtering criteria. At this time, both the key and value must be parsed by software within the associated simulations or humans. Target Modifiers apply to all Target IDs in the Cyber Event.

Because cyber attacks are usually a sequence of events, where each event is predicated on the success of the preceding event, the Cyber DEM doesn't attempt to describe all the events for such an attack in a single structure. Rather, they should be modeled as individual events with the relationship between the events being expressed in federation engineering agreements and linked through the use of Source IDs. Figure 2 illustrates such a sequence.

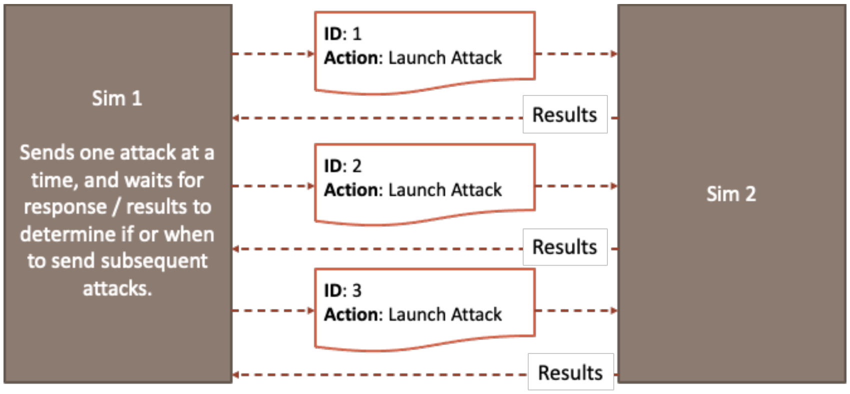
Sim 1
Sends one attack at a time, and waits for response / results to determine if or when to send subsequent attacks.
ID: 1
Action: Launch Attack
Results
ID: 2
Action: Launch Attack
Results
ID: 3
Action: Launch Attack
Results
Sim 2

Figure 2: Sequencing Attacks

Sim 1 launches an attack event bound for execution on Sim 2. Sim 2 receives the request, executes it, and return results. Based on the success or failure reported in those results, Sim 1 decides whether or not to launch the next event in the attack. The reasoning behind Sim 1's decision is federate-specific, but Source IDs in Cyber Event allow the Sim 1 to specify the relationship between the events. In the notional example in Figure 2, the event with ID 2 would have ID 1 as a Source ID, and the event with ID 3 would have ID 2 as a Source ID.

Figure 3 illustrates the Cyber DEM Events model.

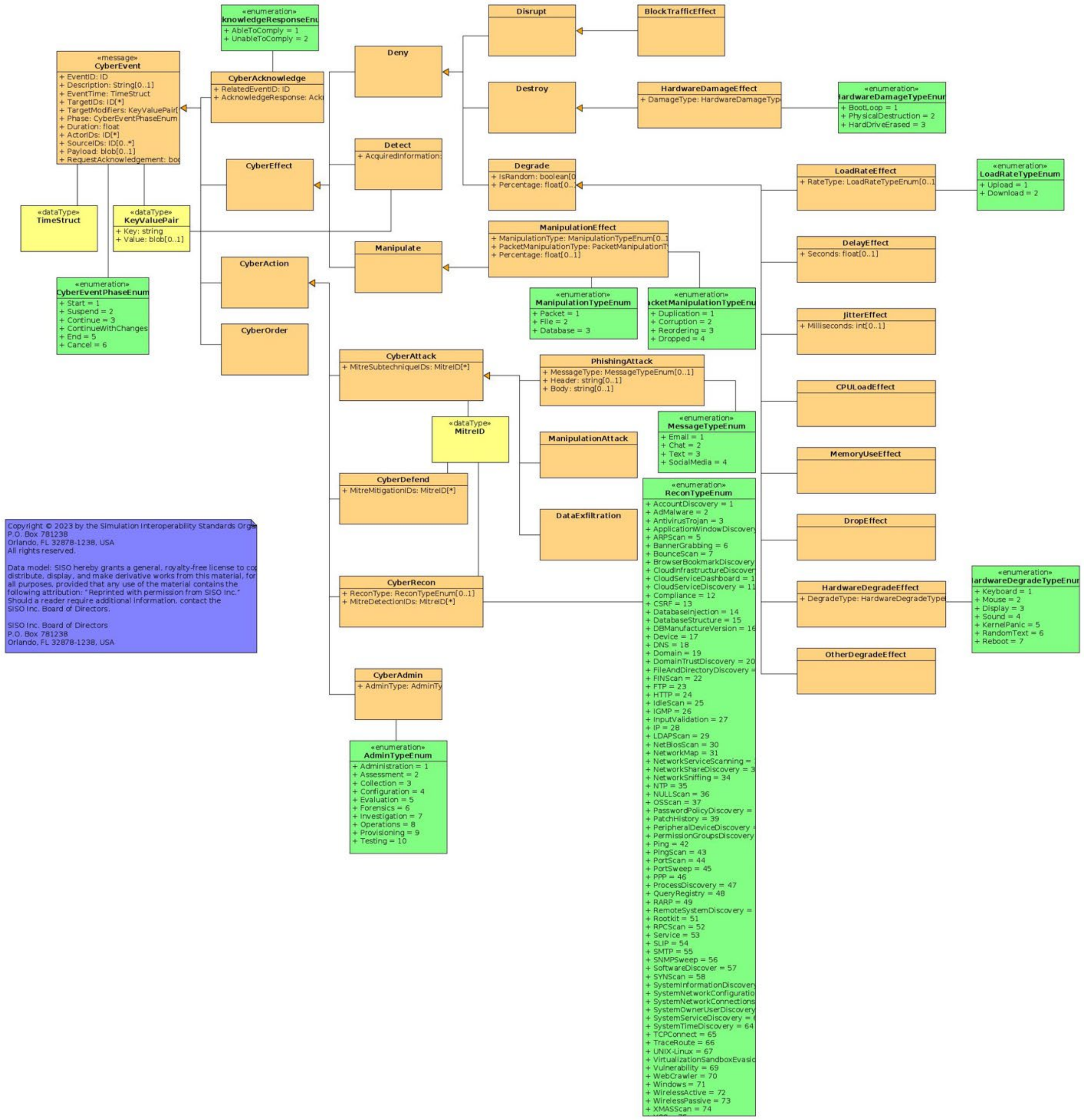

Figure 3: Cyber Events Model

Cyber Event is further decomposed into:

- Cyber Acknowledge
- Cyber Effect
- Cyber Action
- Cyber Order

Each of the subclasses of Cyber Event are described in the following subsections.

6.2.1 Cyber Acknowledge

Cyber Acknowledge represents a response to a Cyber Event that has requested an acknowledgement.

Table 12: Cyber Acknowledge

Attribute	Multiplicity	Description
RelatedEventID		ID of the Cyber Event being acknowledged
AcknowledgeResponse		The response to the related event being acknowledged

6.2.2 Cyber Action

A Cyber Action is the fact or process of doing something, in or through cyberspace, typically to achieve an aim. [Lexico, adapted] Cyber Action is an abstract class intended as an organizational construct; specific effects are instantiated as subclasses.

6.2.2.1 Cyber Admin

Cyber Admin are actions that are administrative in nature and performed by authorized actors.

Table 13: Cyber Admin

Attribute	Multiplicity	Description
AdminType		Type of cyber action of an administration nature (e.g. assessment, collection, and configuration)

6.2.2.2 Cyber Attack

A Cyber Attack is a cyberspace action that creates various direct denial effects in cyberspace (for example, degradation, disruption, or destruction) and manipulation that leads to denial, that is hidden or that manifests in the physical domains [JP3-12].

Techniques represent how an adversary achieves a tactical goal by performing an action. Sub-techniques are a more specific description of the adversarial behavior used to achieve a goal. They describe behavior at a lower level than a technique. Techniques are identified by “T####” and sub-techniques are indicated by the “.###” notation. [ATT&CK v13]

Table 14: Cyber Attack

Attribute	Multiplicity	Description
MitreSubtechniqueIDs	[*]	Reference(s) to MITRE's ATT&CK Sub-technique(s) [ATT&CK v13]; see design pattern 6

6.2.2.2.1 Data Exfiltration

Data Exfiltration is the unauthorized copying, transfer or retrieval of data from a computer or server. Data exfiltration is a malicious activity performed through various different techniques, typically by cybercriminals over the Internet or other network. [Techopedia] Data Exfiltration is an abstract class intended as an organizational construct.

CyberEvent.Target identifies the data being exfiltrated. CyberEvent.ActorID identifies the actor performing the exfiltration.

6.2.2.2.2 Manipulation Attack

A Manipulation Attack controls or changes information, information systems, and/or networks to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification, and other similar techniques. [JP3-12] Manipulation Attack is an abstract class intended as an organizational construct.

6.2.2.2.3 Phishing Attack

A Phishing Attack is the fraudulent practice of sending messages purporting to be from reputable sources in order to induce individuals to reveal sensitive information or unknowingly initiate another attack

Table 15: Phishing Attack

Attribute	Multiplicity	Description
MessageType	[0..1]	Type of the message used in the attack
Header	[0..1]	Message header format is dependent on MessageType (e.g. emails should use IMF (RFC 2822) or MIME; Texts should use SMS or MMS; Chat uses XMPP).
Body	[0..1]	The body/content of the message, format is dependent on the MessageType (e.g. emails should use IMF (RFC 2822) or MIME; Texts should use SMS or MMS; Chat uses XMPP).

6.2.2.3 Cyber Defend

Cyber Defend is a cyberspace action taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach the cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration. [JP3-12]

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed. Mitigations are identified by “M####” notation. [ATT&CK v13]

Table 16: Cyber Defend

Attribute	Multiplicity	Description
MitreMitigationIDs	[*]	Reference(s) to MITRE's ATT&CK Mitigation(s) [ATT&CK v13]; see design pattern 6

6.2.2.4 Cyber Recon

Cyber Recon represents activities in cyberspace conducted to gather intelligence required to support future offensive cyber operations (OCO) or defensive cyber operations (DCO). [FM3-12]

The detect tactic is used to identify adversary access to or unauthorized activity on computer networks. Detect techniques format D3-xxxxx, where “xxx” are the first letters in the technique’s name. [D3FEND]

Table 17: Cyber Recon

Attribute	Multiplicity	Description
ReconType	[0..1]	Type of cyber activity, such as AccountDiscovery, BannerGrabbing, Compliance, etc., conducted to gather intelligence required to support future offensive or defensive cyber operations

Attribute	Multiplicity	Description
MitreDetectionIDs	[*]	Reference(s) to MITRE's D3FEND Detection(s) [D3FEND]; see design pattern 6

6.2.3 Cyber Effect

A Cyber Effect is a change, in or through cyberspace, which is a result or consequence of an action or other cause. [Lexico, adapted] Cyber Effect is an abstract class intended as an organizational construct; specific effects are instantiated as subclasses. Cyber Effect is further decomposed into deny (degrade, destroy, and disrupt) and manipulate consistent with US Joint Publication 3-12 [JP3-12] and detect.

6.2.3.1.1 Degrade

Degrade represets denying access to, or operation of, a target to a level represented as a percentage of capacity. [JP3-12]

Table 18: Degrade

Attribute	Multiplicity	Description
IsRandom	[0..1]	Whether or not the disruption is uniform or random
Percentage	[0..1]	Percentage of degradation (where 100.0 is equivalent to disrupt)

6.2.3.1.1.1 CPU Load Effect

CPU Load Effect is an abstract class intended as an organizational construct.

6.2.3.1.1.2 Delay Effect

Delay Effect represents the increased time for data to travel between two points.

Table 19: Delay Effect

Attribute	Multiplicity	Description
Seconds	[0..1]	Number of seconds to delay delivery of data. If Degrade.IsRandom = TRUE, Seconds is randomized for each packet.

6.2.3.1.1.3 Drop Effect

Drop Effect is an abstract class intended as an organizational construct.

6.2.3.1.1.4 Hardware Degrade Effect

Hardware Degrade Effect represents the degradation but not destruction of hardware.

Table 20: Hardware Degrade Effect

Attribute	Multiplicity	Description
DegradeType	[0..1]	Type of hardware degradation

The percentage the hardware is degraded is inherited from the Degrade parent class.

6.2.3.1.1.5 Jitter Effect

Jitter Effect represents the variance in time delay in milliseconds (ms) between data packets over a network; a disruption in the normal sequence of sending data packets.

Table 21: Jitter Effect

Attribute	Multiplicity	Description
Milliseconds	[0..1]	Time delay variance. If Degrade.IsRandom = TRUE, Milliseconds is randomized for each packet

6.2.3.1.1.6 Load Rate Effect

Load Rate Effect represents the impact on data upload or download rate.

Table 22: Load Rate Effect

Attribute	Multiplicity	Description
RateType	[0..1]	Type (direction) of load that is effected

The percentage the load rate is degraded is inherited from the Degrade parent class.

6.2.3.1.1.7 Memory Use Effect

Memory Use Effect is an abstract class intended as an organizational construct.

6.2.3.1.1.8 Other Degrade Effect

Other Degrade Effect is an abstract class intended as an organizational construct for representing a generic degradation effect.

6.2.3.2 Deny

Deny represents preventing access to, operation of, or availability of a target function by a specified level for a specified time, by degrade, disrupt, or destroy. Deny is an abstract class intended as an organizational construct; specific effects are instantiated as subclasses.

6.2.3.3 Detect

Detect represents discovering or discerning the existence, presence, or fact of an intrusion into information systems. [ATT&CK v13]

Table 23: Detect

Attribute	Multiplicity	Description
AcquiredInformation	[*]	Key-value pairs describing information acquired as a result of a Detect Cyber Effect

6.2.3.3.1 Destroy

Destroy represents completely and irreparably denying access to, or operation of, a target. [JP3-12] Destroy is an abstract class intended as an organizational construct; specific effects are instantiated as subclasses.

6.2.3.3.1.1 Hardware Damage Effect

Hardware Damage Effect represents physical damage to a device.

Table 24: Hardware Damage Effect

Attribute	Multiplicity	Description
DamageType	[0..1]	Type of damage to the hardware

6.2.3.3.2 Disrupt

Disrupt represents completely but temporarily denying access to, or operation of, a target for a period of time. [JP3-12] Disrupt is an abstract class intended as an organizational construct; specific effects are instantiated as subclasses.

6.2.3.3.2.1 Block Traffic Effect

Block Traffic Effect represents completely blocking all traffic over a communication channel. Block Traffic Effect is an abstract class intended as an organizational construct.

6.2.3.4 Manipulate

Manipulate represents the effect of controlling or changing information, information systems, and/or networks to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification, and other similar techniques. [JP3-12] Manipulate is an abstract class intended as an organizational construct.

6.2.3.4.1 Manipulation Effect

A Manipulation Effect describes the type, effected information/system/network, and/or extent (as a percentage) of the manipulation attack.

Table 25: Manipulation Effect

Attribute	Multiplicity	Description
Manipulate	ManipulationType	[0..1]
Manipulate	PacketManipulationType	[0..1]
Manipulate	Percentage	[0..1]

6.2.4 Cyber Order

Cyber Order captures cyberspace related command and control orders/directives. Cyber Order is an abstract class intended as an organizational construct. The commander will need a persona to be represented in the Actor ID. If the order is directed at live subordinates, they will need to have personas to be the targets of the order. The content of the orders is represented in the Target Modifiers.

6.3 Data Structures

6.3.1 Key Value Pair

Key Value Pairs are for specifying additional criteria for targets and Detect Acquired Information.

Table 26: Key Value Pair

Field	Multiplicity	Description
Key		Identification of the criterion for additional filtering
Value	[0..1]	Value of the criterion identified in the key. The datatype is based on the keyword.

6.3.2 Network Interface Struct

Network Interface Struct represents a network interface, hardware and/or software, that enables a device to connect to a network link. A network interface can exist with or without a link, but not without a device.

Table 27: Network Interface Struct

Field	Multiplicity	Description
RelatedObjectID		The identifier of the related object (either a Device or NetworkLink)
Name	[0..1]	The hostname of the device on the network link
Address		A network specific address (e.g. the IP address or URN)

6.3.3 Related Object Struct

Related Object Struct describes properties about a relationship between objects.

Table 28: Related Object Struct

Field	Multiplicity	Description
RelatedObjectID		The identifier of the related CyberObject
RelationshipType	[0..1]	Type of relationship identified between this object and other objects, such as Administer, AdministeredBy, ComponentOf, HasComponent, etc.
RelatedObjectPrivileges	[*]	List of privileges the object with respect to the related object (e.g. a persona might possess privileges specific to a device or application)

6.3.4 Time Struct

Time Struct is a placeholder for simulation time specified in a federation-specific format.

6.3.5 Mitre ID

A (String) ID from the MITRE ATT&CK or D3FEND matrix. Sub-technique IDs are formatted as T####.###. Mitigation IDs are formatted as M####. Detection IDs are formatted as D3-xxxxx.

6.4 Enumerations

The following are the Cyber DEM enumerations at the time the standard was completed. Updates to the enumeration values may occur between versions of the standard via the Enumerations SWG. See the latest version of SISO-REF-010 for the current values.

Acknowledge Response Type - Responses for an acknowledgement

Table 29: Acknowledge Response Type

Name	Value	Description
AbleToComply	1	Able to Comply / Accept
UnableToComply	2	Unable to Comply / Reject

Admin Type - Actions performed on a system

Table 30: Admin Type

Name	Value	Description
Administration	1	Installation, configuration, troubleshooting, and maintenance of systems, networks, data, or accounts
Assessment	2	Determining deviations from acceptable configurations, enterprise, or local policy; determining level of risk; analysis of operational and technical security controls
Collection	3	Collection of data located on the network or system(s) for the purposes of intelligence, assessment, or planning
Configuration	4	Making changes to system, software, security, or network settings
Evaluation	5	Analyzing systems for compliance with specifications and requirements
Forensics	6	Collection, processing, preservation, and/or analysis of computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations
Investigation	7	Analyze information technology (IT) or cybersecurity events related to systems, networks, and digital evidence
Operations	8	Support, administration, or maintenance necessary to ensure effective and efficient information technology (IT) system performance and security
Provisioning	9	Procuring or building IT systems
Testing	10	Execution of all or part of a system to evaluate and verify compliance with specifications or requirements

Cyber Event Phase Type - Execution phase of a cyber event

Table 31: Cyber Event Phase Type

Name	Value	Description
Start	1	Initiate cyber event
Suspend	2	Pause cyber event
Continue	3	Resume paused cyber event
ContinueWithChanges	4	Resume paused cyber event with changes to parameters
End	5	End cyber event regardless of remaining duration
Cancel	6	The cyber event is cancelled regardless of it's current phase

Data Link Protocol Type - Types of data link protocols

Table 32: Data Link Protocol Type

Name	Value	Description
Ethernet	1	IEEE 802.3 networking protocol (based on the Carrier Sense Multiple Access/Collision Detection CSMA/CD protocol), used for connected devices in a wired LAN or WAN

Name	Value	Description
WiFi	2	A capability allowing computers, smartphones, or other devices to connect to the internet or communicate with one another wirelessly within a particular area
ATM	3	Asynchronous transfer mode
LocalTalk	4	A particular implementation of the physical layer of the AppleTalk networking system from Apple Computer
PPP	5	Point-to-point protocol
TokenRing	6	IEEE 802.5, a local area network (LAN) topology that sends data in one direction throughout a specified number of locations by using a token
VLAN	7	Virtual local area network
Bluetooth	8	A short-range wireless technology standard that is used for exchanging data between fixed and mobile devices and building personal area networks (PANs)
1553Bus	9	MIL-STD-1553 multiplex data bus system
LLC	10	Logical Link Control

Data Status Type - Confidentiality, integrity, availability status of data

Table 33: Data Status Type

Name	Value	Description
Intact	1	Data is complete, not damaged or impaired in any way
Compromised	2	Data has been modified or accessed without authorization
Corrupted	3	Data integrity is lost
Manipulated	4	Data has been altered (by unauthorized means)
NonDecryptable	5	Data is encrypted and not accessible by authorized users
Erased	6	Data was deleted and is irretrievable

Data Type - Types of data

Table 34: Data Type

Name	Value	Description
File	1	File in human readable format
Code	2	File in binary format
Credentials	3	File with authentication data, e.g. PKI keys, hashed passwords
Communications	4	Data in motion through a communications channel
SystemConfiguration	5	A system's configuration data (e.g. MS Windows Registry database)

Device Type - Electronic device types

Table 35: Device Type

Name	Value	Description
Generic	1	General device with logic bearing components
Networking	2	Includes routers, switches, VPN concentrators
ComputerNode	3	General purpose computer, e.g. a server or desktop
PortableComputer	4	Computer that is mobile, e.g. a laptop or tablet
Controller	5	Device used to control another device, e.g. a storage device controller
Storage	6	Non-volatile memory device, e.g. thumb drive, solid-state drive, serial advanced technology attachment
Sensor	7	Device that reports certain conditions, e.g. environmental, operating status
Printer	8	Device for producing printed output including paper and 3D materials
Scanner	9	Device for producing a digital representation of a physical item, e.g. printed material, fingerprint, facial recognition, highway toll readers
Communications	10	Device that performs non-computer communications, e.g. radio, telephone, cellular
HMI	11	Human machine interface. Devices through which the user interacts with a computer system
Monitoring	12	Software that inspects digital actions, e.g. Intrusion Detection Systems (IDS)
IoT	13	Internet of things. Device that uses internet protocols for communications, command and control
Security	14	Device that provides security functions to the system

Encryption Type - Type of encryption used for data

Table 36: Encryption Type

Name	Value	Description
NotEncrypted	1	No encryption used
DES	2	Data encryption standard
TripleDES	3	Triple DES
RSA	4	Rivest Shamir Adleman
AES	5	Advanced encryption standard
TwoFish	6	Twofish encryption

Hardware Damage Type - Type of physical damage rendered by a hardware damage cyber effect

Table 37: Hardware Damage Type

Name	Value	Description
BootLoop	1	Repeated, uninterruptable rebooting
PhysicalDestruction	2	Physical damage to hardware, e.g. overheating
HardDriveErased	3	Hard drive is not readable, e.g. zeroized or file allocation table erased

Hardware Degrade Type - Type of degradation effect to hardware

Table 38: Hardware Degrade Type

Name	Value	Description
Keyboard	1	Keyboard inoperable or degraded performance
Mouse	2	Mouse inoperable or degraded performance
Display	3	Display inoperable or unreadable
Sound	4	Sound inoperable

Load Rate Type - Which direction of data transfer is impacted by a load rate cyber effect

Table 39: Load Rate Type

Name	Value	Description
Upload	1	Slow upload toward the target
Download	2	Slow download from the target

Manipulation Type - Type of effect achieved by a manipulation cyber effect

Table 40: Manipulation Type

Name	Value	Description
Packet	1	Communications packets
File	2	Files on a drive/system
Database	3	Database records

Message Type - Message vector for phishing attacks

Table 41: Message Type

Name	Value	Description
Email	1	Contents of an email
Chat	2	Two way non-voice communication through an application hosted on any device
Text	3	Two way non-voice communication through a cellular device
SocialMedia	4	Data published on a social media platform

Network Protocol Type - Types of network protocols

Table 42: Network Protocol Type

Name	Value	Description
InternetProtocol	1	Internet protocol
NAT	2	Network address translation
ICMP	3	Internet control message protocol
ARP	4	Address resolution protocol
RIP	5	Routing information protocol
OSPF	6	Open shortest path first
IPsec	7	Internet protocol security

Operating System Type - Types of operating systems

Table 43: Operating System Type

Name	Value	Description
MicrosoftDOS	1	Microsoft's Disk Operating System
MicrosoftWindows	2	Microsoft's OS with a Windowing UI
AppleMacOS	3	Apple's OS with a Windowing UI
DECVMS	4	Digital Equipment Corporation Virtual Memory System
IBMOS_2	5	International Business Machines OS2
Android	6	Google's mobile phone OS
AppleiOS	7	Apple's mobile phone OS
CiscoIOS	8	Cisco's OS for routers and switches
Firmware	9	Hardware control software
UNIX-Linux	10	Any *nix operating system

Packet Manipulation Type - Type of effect achieved by a packet manipulation cyber effect

Table 44: Packet Manipulation Type

Name	Value	Description
Duplication	1	Sending the same packet again
Corruption	2	Manipulating data within the packet
Reordering	3	Changing the order of packets
Dropped	4	Preventing packets from reaching the destination

Physical Layer Type - Types of network at the physical layer

Table 45: Physical Layer Type

Name	Value	Description
Wired	1	Wired, e.g. ethernet
Wireless	2	Wireless, e.g. IEEE 802.11

Recon Type - The list of types for recon actions

Table 46: Recon Type

Name	Value	Description
AccountDiscovery	1	Identify accounts
AdMalware	2	Host-based scan
AntivirusTrojan	3	Host-based scan
ApplicationWindowDiscovery	4	Identify open application windows
ARPScan	5	Address Resolution Protocol scan
BannerGrabbing	6	Web application scan
BounceScan	7	Transport layer - TCP scan
BrowserBookmarkDiscovery	8	Identify bookmarks
CloudInfrastructureDiscovery	9	Identify resources that are available in an IaaS
CloudServiceDashboard	10	Identify resources available via compromised credentials
CloudServiceDiscovery	11	Identify cloud services running
Compliance	12	Host-based scan (PICDSS, HIPAA, ISO 27001, NIST SP800.53)
CSRF	13	Cross site request forgery scan
DatabaseInjection	14	Database enumeration (Boolean-based blind, time-based blind, error based, union query, stacked query, out-of-band), scans to test for vulnerabilities not actual exploiting
DatabaseStructure	15	Database enumeration - tables, columns, users, privileges, roles
DBManufactureVersion	16	Database enumeration
Device	17	Identify devices
DNS	18	Identify Domain Name System
Domain	19	Identify domains
DomainTrustDiscovery	20	Identify domain trust relationships
FileAndDirectoryDiscovery	21	Identify file and directory structure
FINScan	22	Transport layer - TCP scan
FTP	23	File transfer protocol scan
HTTP	24	Hyper text transfer protocol scan

Name	Value	Description
IdleScan	25	Transport layer - TCP scan
IGMP	26	Internet group management protocol scan
InputValidation	27	Application scan (code injection, fuzzing)
IP	28	Internet Protocol scan
LDAPScan	29	Lightweight directory access protocol scan
NetBiosScan	30	Identify NetBios enabled systems
NetworkMap	31	Determine topology
NetworkServiceScanning	32	Identify network services running
NetworkShareDiscovery	33	Identify shared folders and drives
NetworkSniffing	34	Capture network traffic for analysis
NTP	35	Network Time Protocol scan
NULLScan	36	Transport layer - TCP scan
OSScan	37	Identify operating systems
PasswordPolicyDiscovery	38	Identify password policy
PatchHistory	39	Host-based scan
PeripheralDeviceDiscovery	40	Identify devices connected to a computer system
PermissionGroupsDiscovery	41	Identify group permissions
Ping	42	Single host
PingScan	43	Multiple host
PortScan	44	Single host, multiple ports
PortSweep	45	Multiple hosts, single port
PPP	46	Point-to-point protocol scan
ProcessDiscovery	47	Identify processes running on the system
QueryRegistry	48	Gather registry information
RARP	49	Reverse address resolution protocol scan
RemoteSystemDiscovery	50	Identify remote systems
Rootkit	51	Host-based scan
RPCScan	52	Remote Procedure Call scan
Service	53	Identify active services
SLIP	54	Serial line internet protocol scan
SMTP	55	Simple mail transfer protocol scan
SNMPSweep	56	Simple network management protocol scan
SoftwareDiscover	57	Identify installed software
SYNScan	58	Transport layer - TCP scan

Name	Value	Description
SystemInformationDiscovery	59	Identify operating system version and patch level
SystemNetworkConfigurationDiscovery	60	Identify network configuration
SystemNetworkConnectionsDiscovery	61	Identify network connections
SystemOwnerUserDiscovery	62	Identify primary user / currently logged in user
SystemServiceDiscovery	63	Identify registered services on the system
SystemTimeDiscovery	64	Identify system time and time zone
TCPConnect	65	Transmission Control Protocol scan
TraceRoute	66	Network route to system
UNIX-Linux	67	Identify *nix OS
VirtualizationSandboxEvasion	68	Identify virtualization/analysis environment
Vulnerability	69	Host-based scan
WebCrawler	70	Web application scan
Windows	71	Identify Windows OS
WirelessActive	72	Wireless network scan
WirelessPassive	73	Wireless network scan
XMASScan	74	Transport layer - TCP scan
XSS	75	Cross site scripting scan

Relationship Type - Describes relationships between cyber objects

Table 47: Relationship Type

Name	Value	Description
Administers	1	The citing object administers the cited object
AdministeredBy	2	The citing object is administered by the cited object
ComponentOf	3	The citing object is a component of the cited object
HasComponent	4	The citing object has the cited object as a component
ContainedIn	5	The citing object is contained in the cited object
Contains	6	The citing object contains the cited object
ProvidedBy	7	The citing object is a provided by the cited object
Provides	8	The citing object provides the cited object
ResidesOn	9	The citing object resides on the cited object
HasResident	10	The citing object has resident of the cited object

Sensitivity Type - Classification, releasability, and sensitivity designations for data; see US DoD 5200.1-PH; US HHS CFR 46 parts 160, 162, and 164; US DOL Guidance on the Protection of Personal Identifiable Information; EU General Data Protection Regulation

Table 48: Sensitivity Type

Name	Value	Description
Unclassified	1	No classification
Confidential	2	Public disclosure would damage national security
FOUO	3	For official use only
Secret	4	Public disclosure would cause serious damage to national security
SecretNoForn	5	Secret / restricted to country of source
TS	6	Top secret, unauthorized disclosure would cause exceptionally grave damage to national security
TS_SCI	7	Top secret / Sensitive compartmented information
NATORestricted	8	North Atlantic Treaty Organization Restricted
NATOConfidential	9	North Atlantic Treaty Organization Confidential
NATOSecret	10	North Atlantic Treaty Organization Secret
CosmicTopSecret	11	Top Secret documents managed by a COSMIC registry.
FVEYProprietary	12	Five eyes proprietary
Proprietary	13	Information a company wishes to keep confidential (e.g. trade secrets)
PII	14	Personal identifiable information
HIPAA	15	Health information portability and accountability act
GDPR	16	General data protection regulation
Public	17	Unrestricted/open to the public
CUI	18	Controlled Unclassified Information

Service Type - Types of application services

Table 49: Service Type

Name	Value	Description
DNS	1	Domain Name System
Email	2	Service that transmits and receives electronic mail messages (typically using SMTP)
Web	3	Service that hosts web pages and provides them via HTTP/HTTPS
Database	4	Service that stores and manages data (e.g. RDBMS)
File	5	Service that provides files to remote devices on a network
Chat	6	Service that allows users to exchange short messages (e.g. IRC)
Forum	7	Service that allows users to share information and collaborate about a particular topic

Name	Value	Description
SocialMedia	8	Website and/or application that enables users to create and share content or to participate in social networking.
Containerization	9	Service that packages libraries, frameworks, and applications into an isolated execution environment utilizing shared resources on a host platform
Virtualization	10	Technology that simulates physical hardware and represents it as a separate virtual machine (VM)
NetworkTime	11	Network protocol for clock synchronization between connected devices (e.g. NTP)

System Type - Types of systems other than those specified by Device Type

Table 50: System Type

Name	Value	Description
Generic	1	Non-DeviceType system other than SCADA, CT, or ICS
SCADA	2	Supervisory control and data acquisition
C2	3	Command and control
ICS	4	Industrial computer system

7 Use Cases

This section provides examples of rendering data exchanges from the original use cases into the Cyber DEM in a simulation interoperability solution-neutral representation. Simulation interoperability solution-specific representations of these examples are provided in the solution-specific subsections of section 8.

7.1 COBWebS

This use case from COBWebS targets all inbound Variable Message Format (VMF) (MIL-STD-6017) free text (K01.1) messages to two specific Joint Battle Command Platform (JBC-P) terminals. This is an example of defining a Cyber Event that contains target information expressed using key-value pairs. Because targeting with this level of specificity is not currently supported natively by the Cyber DEM, allowable values for the key-value pair contents, e.g. Message Type, Direction, and Designator, must be specified in federation agreements.

Assuming the Object ID of JBC-P terminal 1 is 285 and the Object ID of JBC-P terminal 2 is 312, the Cyber Event would be:

TargetIDs[0]: 285

TargetIDs[1]: 312

TargetModifiers[0]: “MessageType”: “MIL-STD-6017”

TargetModifiers[1]: “Direction”:“inbound”

TargetModifiers[2]: “Designator”:“K01.1”

7.2 CyberBOSS

This use case from CyberBOSS illustrates a blue force commander ordering cyber forces to execute reconnaissance of the adversary’s network. As a result, blue cyber forces report the discovery of the WiFi in a cyber café.

Assuming:

- The Object ID of the blue cyber force Device is 79.
- The Object ID of the adversary Network is 86.
- The recon occurs at 0500 UTC and the time representation used by the overall federation is an integer representation of UTC.
- The recon takes an hour and the time representation used by the overall federation is an integer representation of minutes.
- The recon will be achieved through network mapping.
- The Object ID of the cyber café WiFi NetworkLink is 54.
- The recon takes 23 minutes.
- The desired information is the SSID of the cyber café WiFi.

The Cyber Recon event would be:

ActorIDs[0]: 79

EventTime: 500

TargetIDs[0]: 86

Phase: Start

Duration: 60

ReconType: NetworkMapping

The Detect event would be:

ActorID[0]: 79

TargetIDs[0]: 54

EventTime: 523

AcquiredInformation[0]: “SSID”: “Brew-n-bytes”

7.3 TENA Retina

TENA Retina is a visualization tool focused on providing cyber white cell teams visibility into cyber actions and the cyber environment during a test or training event. Here is a use case from a recent training event:

1. Red Team initiates a scan on Blue Team assets. The CyberAttack event would be:

   ActorID[0]: Red Team Name

   MitreAttackSubtechniqueIDs[0]: “T1046”

   TargetID[0]: Network segment(s) under scans (e.g. 192.168.110.0/24)

   TargetModifier[0]: “Tactic”: “Discovery”

   TargetModifier[1]: “Technique”: “Network Service Scanning”

   TargetModifier[2]: “Port(s)”: “3389, 445, 22, 111”

   Phase: Start

2. Blue Team identifies suspicious activity. The CyberDefend would be:

   ActorID[0]: Blue Team Name

   TargetID[0…n]: Network segment(s) detected (e.g. 192.168.110.111…n)

   TargetModifier[0]: “Tactic”: “Detect”

TargetModifier[1]: “Technique”: “Remote System Discovery”

TargetModifier[2]: “Port(s)”: “3389, 445, 22, 111”

Phase: Start

3. Blue Team investigates suspicious activity. The CyberDefend would be:

ActorID[0]: Blue Team Name

TargetID[0…n]: Network segment(s) detected (e.g. 192.168.110.111…n)

TargetModifier[0]: “Tactic”: “Discovery”

TargetModifier[1]: “Action”: “CSSP checking reputation of 196.87.105.83”

Phase: Continue

4. Blue Team takes defensive action. The CyberDefend would be:

ActorID[0]: Blue Team Name

MitreAttackMitigationID[0]: M1031

TargetID[0…n]: Network segment(s) detected (e.g. 192.168.110.111…n)

TargetModifier[0]: “Tactic”: “Deny”

TargetModifier[1]: “Mitigation”: “Network Intrusion Prevention”

TargetModifier[2]: “Action”: “Identified and blocked RDP and SSH connections from outside network (196.87.105.83)”

Phase: End

5. Red Team confirms or denies Blue Team’s findings. The CyberAttack event would be:

ActorID[0]: Red Team Name

MitreAttackSubtechniqueIDs[0]: T1046

TargetID[0]: Network segment(s) under scans (e.g. 192.168.110.0/24)

TargetModifier[0]: “Tactic”: “Discovery”

TargetModifier[1]: “Technique”: “Network Service Discovery”

TargetModifier[2]: “Action”: “Match. Scans confirmed on 3389, 445, 22, 111.”

Phase: End

8 Mapping the Cyber DEM to Existing Interoperability Solutions

This section provides general guidance for mapping the Cyber DEM to specific interoperability solutions. With the Cyber DEM standardized, solution-specific DEMs will be developed. The HLA and TENA versions will be standardized through SISO. The DIS version will be standardized through IEEE. The JSON version is provided with the Cyber DEM as a product data file.

Code examples derived from the use cases in sections 7.1 and 7.3 rendered in HLA and TENA respectively will be provided as SISO Product Data Files (https://www.sisostds.org/Schemas.aspx).

8.1 High Level Architecture (HLA)

Cyber Object and its derived classes map to HLA objects with the same inheritance hierarchy. Cyber Event and its derived classes map to HLA interactions with the same inheritance hierarchy. Pursuant to design pattern 2, the Cyber DEM will become a modular FOM per IEEE 1516-2010 and subsequent versions. This will directly enable inheritance of classes such as time and duration. Table 51 details how datatypes in the Cyber DEM are mapped to HLA datatypes.

Table 51: Cyber DEM to HLA Datatype Mapping

Cyber DEM	HLA
blob	HLAopaqueData
boolean	HLAboolean
enumeration	As specified in the enumerated datatype table; typically HLAinteger32BE
float	HLAfloat64BE
int	HLAinteger64BE
ObjectID	HLAfixedRecord with a single field of type HLAASCIIstring
string	HLAASCIIstring

8.2 Distributed Interactive Simulation (DIS)

Cyber Object and its derived classes will require creation of a new PDU in the Information Operations protocol family. Cyber Event and its derived classes will require record enhancements to the existing Information Operations Action and Report PDUs. Table 52 details how datatypes in the Cyber DEM are mapped to DIS datatypes.

Table 52: Cyber DEM to DIS Datatype Mapping

Cyber DEM	DIS
blob	A record that consists of each individual character as an 8-bit unsigned integer and number of characters as a 16-bit unsigned integer
boolean	1-bit Boolean
enumeration	32-bit enumeration (unsigned integer)
float	64-bit floating point
int	64-bit integer
ObjectID	Entity Identifier which consists of three 16-bit unsigned integers that are referred to as Site Number, Application Number, and Entity Number
string	A record that consists of each individual character as an 8-bit unsigned integer and number of characters as a 16-bit unsigned integer

8.3 Test & Training Enabling Architecture (TENA)

Draft TENA Definition Language files for Cyber Object and Cyber Event have been created and will be managed as part of the TRMC User Group. All TENA Definition Language (tdl) files, auto-generated code, and protypes will be maintained and managed at https://www.trmc.osd.mil/wiki/display/CyberDEM/CyberDEM+Home.

Table 53 details how datatypes in the Cyber DEM are mapped to TENA datatypes.

Table 53: Cyber DEM to TENA Datatype Mapping

Cyber DEM	TENA
blob	A TENA local class encompassing native types and binary data
boolean	bool
enumeration	TENA::Enumeration
float	TENA::float64
int	TENA::int64
ObjectID	SDO or Message ID
string	TENA::string

8.4 JavaScript Object Notation (JSON)

The Cyber Object, Cyber Event, and their derived classes will be constructed using the ECMA-404 specification for JSON to ensure compatibility with older applications. The JSON specification provides native support for a few simple datatypes (e.g.; boolean, number, string, null, and undefined) and complex datatypes (e.g.; object and array). The JSON schema will define the custom datatypes that are needed to support the Cyber DEM (i.e.; ObjectID). Table 54 details how datatypes in the Cyber DEM are mapped to JSON datatypes.

Table 54: Cyber DEM to JSON Datatype Mapping

Cyber DEM	JSON
blob	base64 encoded string
boolean	boolean
enumeration	string (UTF-16)
float	number (double-precision 64-bit binary format IEEE 754)
int	number (double-precision 64-bit binary format IEEE 754)
ObjectID	An Entity Identifier will be constructed to define the ObjectID. The Entity Identifier will include a Site Number, Application Number, and Entity Number. The site number will be a number assigned to the site of the application. The application number will be the number assigned to the application. The entity number will be a number assigned to the entity by the application: string (UTF-16).
string	string (UTF-16)