Attacks on C2 Sensor data

# Identification

Use Case ID: <assigned by Cyber M&S SG>

Description: Integrating cyber as a component in Situational Awareness (SA) applications can increase the training audience’s understanding of cyber effects and of considerations that may apply when choosing to deploy (or not to deploy) cyber capabilities.

The following simulation abilities are required:

1. Ability to integrate cyber effects in the radio communication simulation
2. Ability to initiate cyber effects in the radio communication simulation
3. Ability to integrate simulated cyber effects into main exercise simulation engine
4. Ability to emulate cyber capabilities in simulations
5. Ability to simulate effects of cyberattacks on SA applications and the messages they exchange
6. Ability to offer compare effectiveness of selected Course of Actions (CoAs)

Domain: Training

Table 1. POCs

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Organization** | **Role** | **Email** |
| Bert Boltjes | Netherlands Organisation for Applied Scientific Research (TNO) | Originator | bert.boltjes@tno.nl |
| Tom van den Berg | TNO | Originator | tom.vandenberg@tno.nl |

Table 2. Change Log

|  |  |  |
| --- | --- | --- |
| **Version #** | **Date** | **Changes** |
| 0.1 | 12/29/2020 | * Initial draft |

Relationship to other use cases: **TBD**

* <use case ID> - <Description of relationship>

# Goals and Measures of Performance (MOPs)

Training objectives may include, but are not restricted to:

## Goals

1. Improve the training audience’s awareness that communication between Battle Management Systems (BMSs) is vulnerable to manipulation and that the data displayed may not necessarily be correct.
2. Improve the training audience’s response to the suspicion that their BMS might be under attack.
3. Offer CoAs and study the consequences on achieving mission goals and success.

## Measures of Performance (MOPs)

1. Detection rate and detection time
2. Number of effected position reports
3. Discrepancy between actual position/time and reported position/time of each BMS

## Goal / MOP Crosswalk

Table 2. MOPs for Measuring Achievement of Goals

|  |  |
| --- | --- |
| Goal 1 | MOP 1, 2 |
| Goal 2 | MOP 2, 3 |
| Goal 3 | MOP 3 |

# Scenarios Envisioned

In the operational view shown in Figure 1 below, the training audience consists of the operators of Battle Management Systems (on board of each vehicle) and the HQ C2 System. The Battle Management Systems (BMS) exchange position reports through radio communication in order to create and maintain a situational awareness. The commander vehicle reports positions to the HQ C2 System, from where the reports can be distributed to partner HQ C2 Systems as Friendly Force Tracking (FFT) messages[[1]](#footnote-1).

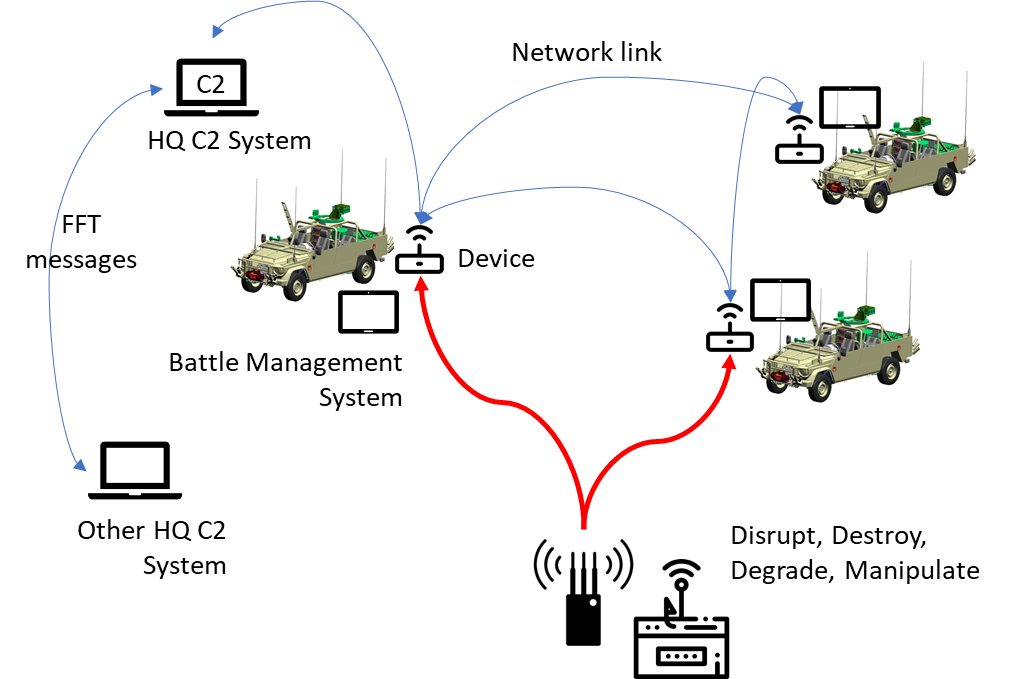


Figure 1: Operational view.

Plausible cyber effects due to attacks that could occur in reality, that should be supported in this use case are i.e.:

* Due to Information Operations:
  + GPS signal blocking
  + Jamming of the local radio link
  + Spoofing of Non-military GPS: malicious displacement of reported friendly forces.
  + Fake FFT reports introduced over the radio link (for the FM9000 this could be possible in the future)
* Due to successful cyberattacks on the HQ C2 System:
  + Delay of FFT messages (randomly)
  + Removal of FFT messages (randomly)
  + Create duplicate (ghost) FFT messages with fictitious positions (flooding with ghost tracks)

Enemy cyber and/or information operations can in potential successfully breach into the tactical C2 network by compromising the integrity of the BMS or C2 System, underlying operating systems, and/or by hijacking the radio link and inject falls messages.  
  
The trainee can be trained to:

* 1. Detect this breach and determine the opponents intentions,
  2. Learn to work with the compromised system,
  3. Abandon the digital BMS or C2 system and switch to backup methods (other sensor data/C2 system, radio call, etc).
  4. Use knowledge of enemy surveillance for deception, i.e. can the opponent’s cyber advantage converted into an own advantage in the physical battlefield?

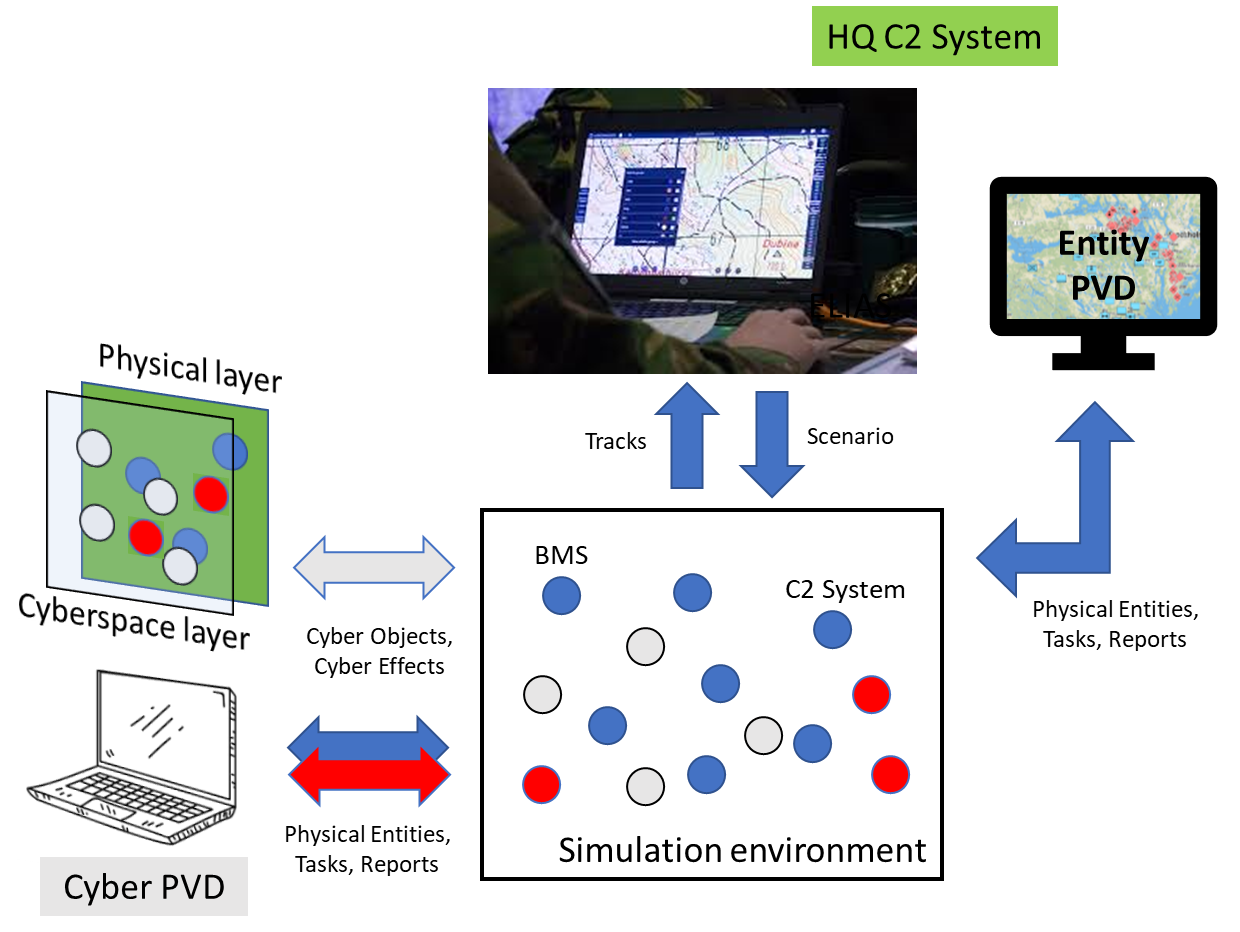
# Conceptual Model

*To be done***.**

# Potential Components

Figure 2 provides a conceptual view of the simulation environment. Main actors (in this simplified view) are the HQ C2 System operator and the Cyber Plan View Display (PVD) operator. The C2 Operator uses his organic C2 system to prepare a simulation scenario and initialize the simulation environment with this scenario. The scenario consists of the own (blue force) units and platforms. The own units/platforms are tasked from an Entity Cyber PVD interface. Tasks and reports are defined in NETN-ETR[[2]](#footnote-2).

The Cyber PVD Operator creates and initializes the simulation environment with the red-force scenario, and injects cyber effects into the simulation environment via a Cyber PVD. The presence of red forces is optional. The Cyber PVD provides several layers of information, amongst others a physical layer showing the physical simulation entities (typically overlaid on a map), and a Cyberspace layer with the Cyber objects.



# **Figure 2: Conceptional view of the cyber effect simulation environment.**

Figure 2 provides a conceptional view of the cyber effects simulation environment based on the NLD FFT simulation environment as was demonstrated at CWIX-2020. All simulation components are NETN-compliant[[3]](#footnote-3).

# 

# Figure 3: System view of the simulation environment.

Simulation components are:

* ORBAT Server: component for posting/publishing a simulation scenario in the simulation environment (as NETN-ORG).
* Entity PVD: component for entity tasking and reporting (no data exchange shown in order to not clutter the picture too much).
* CGF: component for the generation of physical entities (red and/or blue).
* Report Simulator: component for the simulation of the radio networks, including the processing of cyber effects on the radio communication.
* FFT Gateway and Hub: components for processing ADatP-36 standard messages.
* Cyber PVD: component for tasking/reporting of red units/platforms, and for injecting cyber effects into the simulation. Component provides several layers of information. The information and actions offered in the Cyber PVD include:
* View physical entities (RPR-Physical and NETN-Physical)
* Send tasks and view task reports (NETN-ETR)
* View Cyber Objects (SISO CyberDEM)
* Inject Cyber Events (SISO CyberDEM)

# The Report Generator consumes RPR and NETN-Physical entities, NETN-ORG scenario data, and CyberDEM Events. It produces: FFT Reports and CyberDEM Objects. The Generator processes and maintains a network node for each entity in the ORBAT and a so-called “Datalink node” for connections between devices in the nodes. It publishes nodes as Cyber Objects which are used by the Cyber PVD for injecting events. The Cyber effects concern currently:

# BlockTrafficEffect (Disrupt)

# HardwareDamageEffect (Destroy)

# LoadRateEffect, JitterEffect, DelayEffect (Degrade)

# Additional effects, such injecting ghost position reports, may be added in the future.

# In terms of reusability (in the context of Cyber) most interesting is the **Cyber PVD**, as a generic component that can be used in different simulation environments that use the CyberDEM and NETN FOMs.

# Other interesting components are the following, each with a potential future addition:

* **ORBAT Server**: include Cyber elements in simulation scenario (MSDL, NETN-ORG, or possibly C2SIM based schemas).
* **Report Simulator**: add support for NETN-COM in order to separate out the radio network connectivity (including handling of cyber effects) from the actual position reporting logic.

# Derived Data Exchange Model (DEM) Requirements

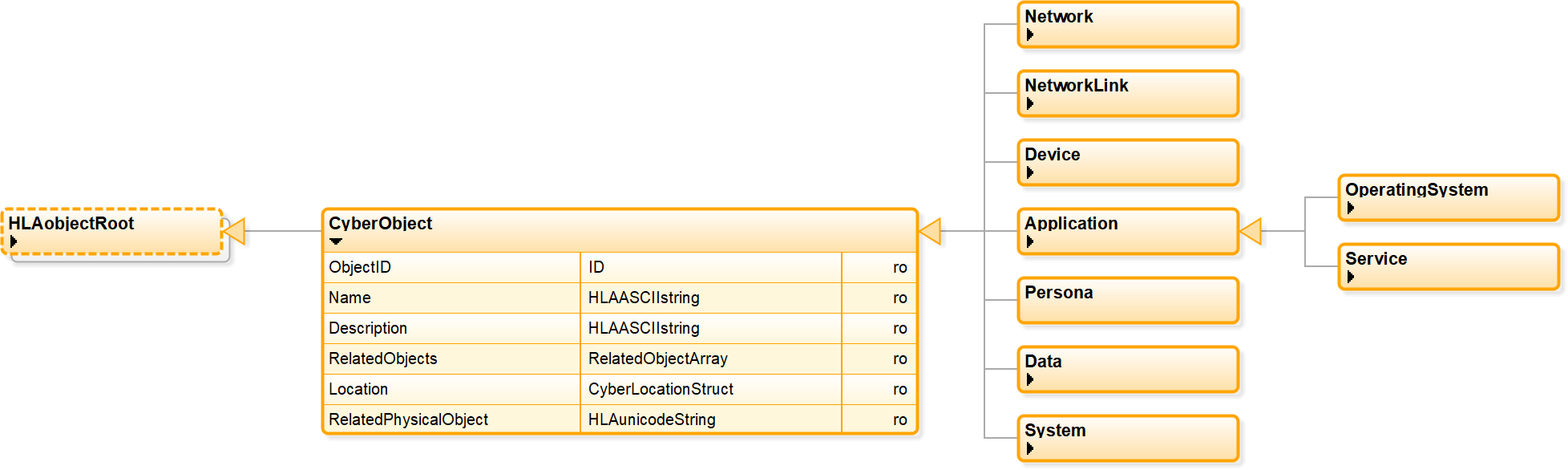
Requirements for FFT Cyber simulation environment:

* Represent Cyber Objects and Cyber Events (to represent C2 and BMS Systems, Network nodes and Data Links).
* Represent relationships between Cyber Objects and Physical entities, and location of Cyber Objects in the physical world.
* Obtain the status of a specific Cyber event (i.e. in progress, completed).
* Cancel a specific Cyber event in progress.
* Obtain all Cyber events in progress.
* Cancel all Cyber events in progress.
* Query a specific Cyber Object for allowed/supported Cyber Event types.
* Uniquely identify Cyber Objects/Events with a UUID.
* Reflect actual effect data in the Cyber Object, based on requested effect data in the Cyber Event.

# Notes, Anomalies, Challenges

* The proposed simulation environment is exploratory. Specific requirements on desired effects still need to be determined in more detail. Limited number of effects used so far.
* Missing relationship between Cyber Objects and Physical Entities.

“Location” and “RelatedPhysicalObject” have (provisionally, as quick work-around) been added to the CyberObject in the CyberDEM as shown in Figure 4:



# Figure 4: Objects added to the CyberDEM.

# References

1. <https://www.act.nato.int/cwix>

# Acronyms

BMS Battle Management System

C2 Command and Control

FFT Friendly Force Tracking

1. NATO ADatP-36 standard. [↑](#footnote-ref-1)
2. https://github.com/AMSP-04 [↑](#footnote-ref-2)
3. https://github.com/AMSP-04 [↑](#footnote-ref-3)