

CYBER M&S V2348

Cyber Modelling & Simulation

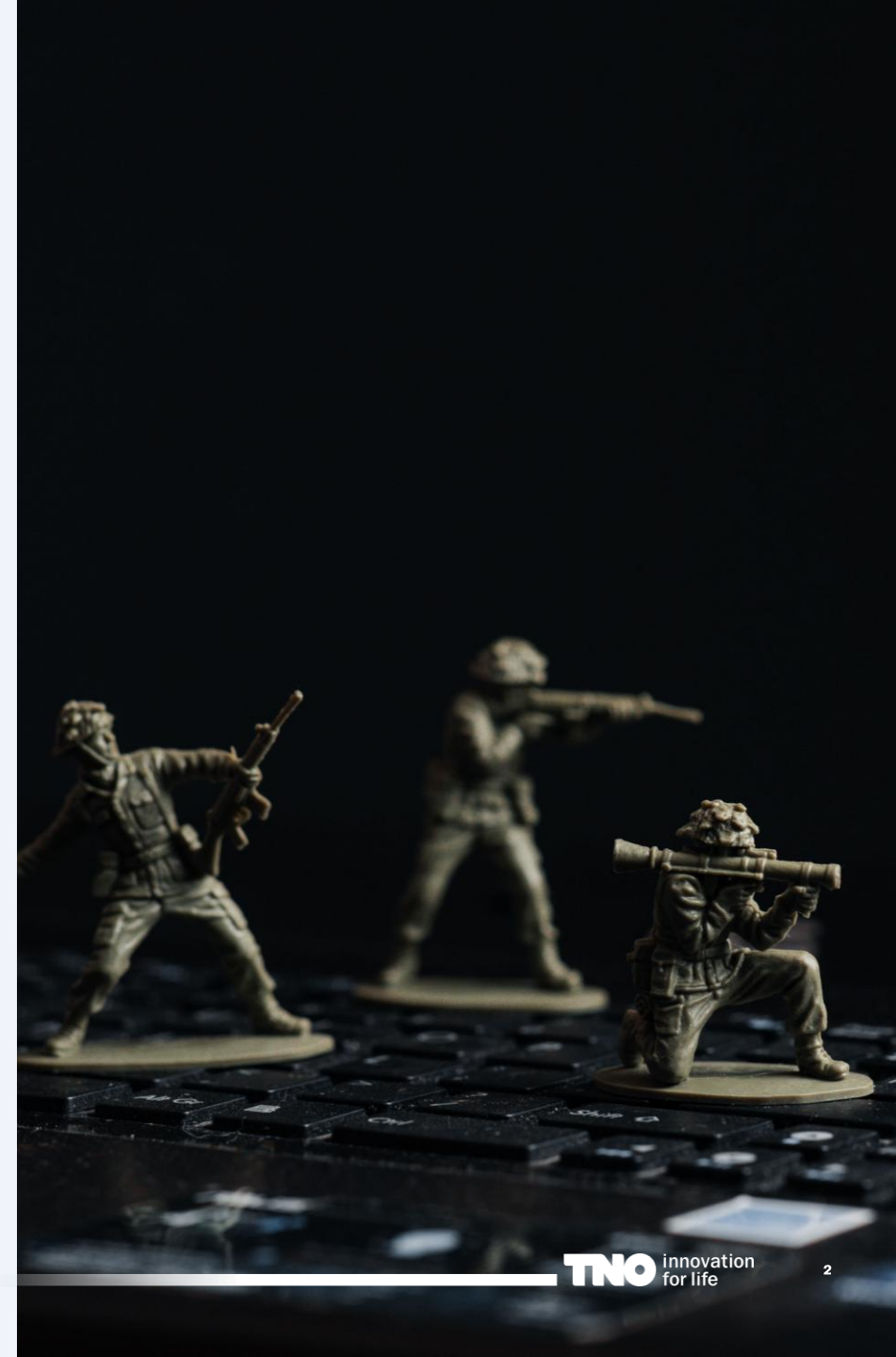
Patrick Darwinkel, Jean Paul Dingemanse



Het programma

“Het vergroten en verbeteren van de operationele mogelijkheden en inzetbaarheid van Cybereffecten in militaire operaties middels ondersteuning door Modelling en Simulatie kennis en capaciteiten.”

- Cyber Warfare and Training Centre (CWTC)
- Verschillende doelgroepen
 - Cyber for cyber
 - Cyber for non-cyber warriors
- Een initiërende rol voor Defensie
 - Onderzoek
 - Ondersteuning
 - Ontwikkeling



Doel van deze workshop

- Indruk van de ervaringen met cyber voor niet-cyber specialisten.
- Wat zijn de behoeftes voor Defensie?
- Kunnen we de overlap in behoeften tussen verschillende defensie onderdelen vinden?
- Aan de hand van bestaande usecases.

Jullie kijk op cyber

- Hoe bewust zijn we van onze digitale kwetsbaarheid?
- Ervaring met systemen die kwetsbaar zijn voor cyberaanvallen?
 - Bijvoorbeeld lessen uit Oekraïne
- Ervaring met cyber in training?
- Voor welke type cyber aanvallen zijn we binnnen onze werkzaamheden kwetsbaar?

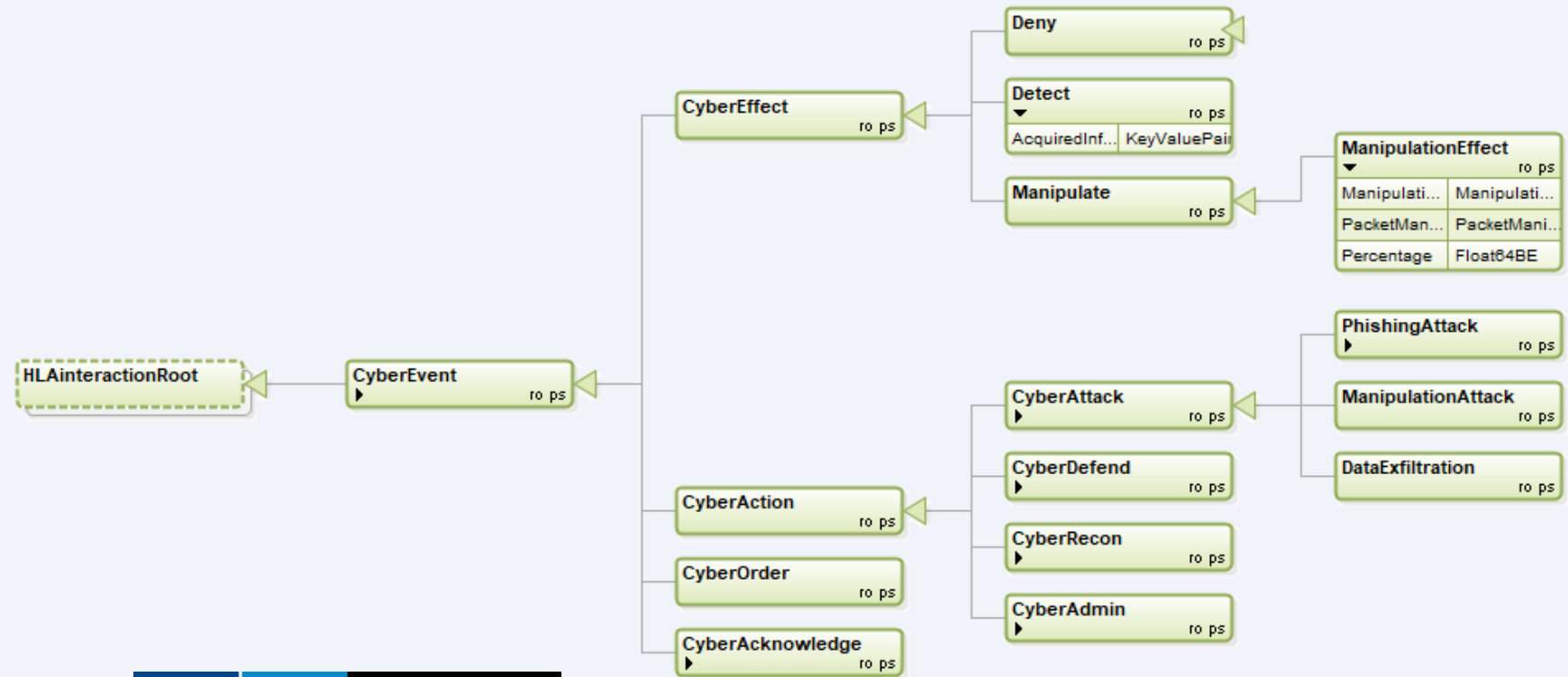


Verschillende use cases

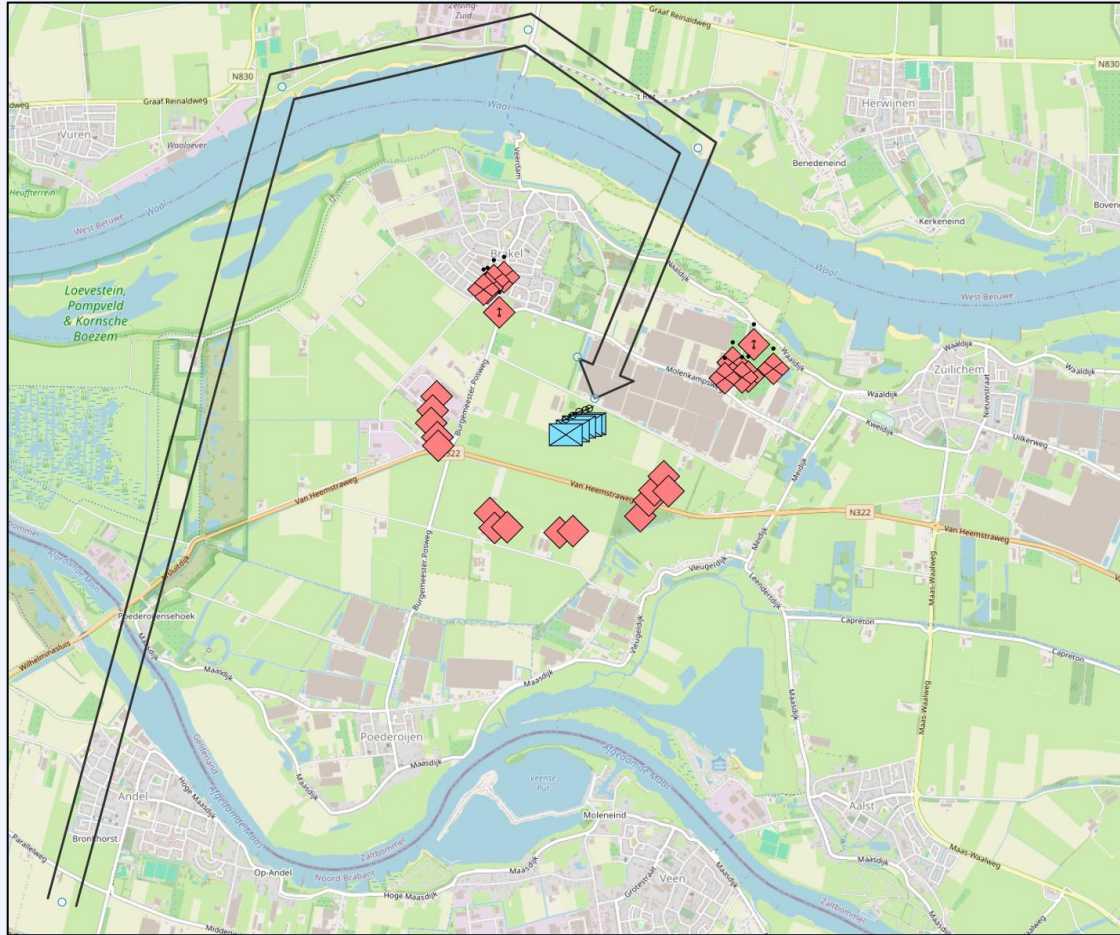
- Cyber bewustzijn
- Cyber concept ontwikkeling
- Interoperabiliteit
- Bestaande tools evalueren

Standaarden

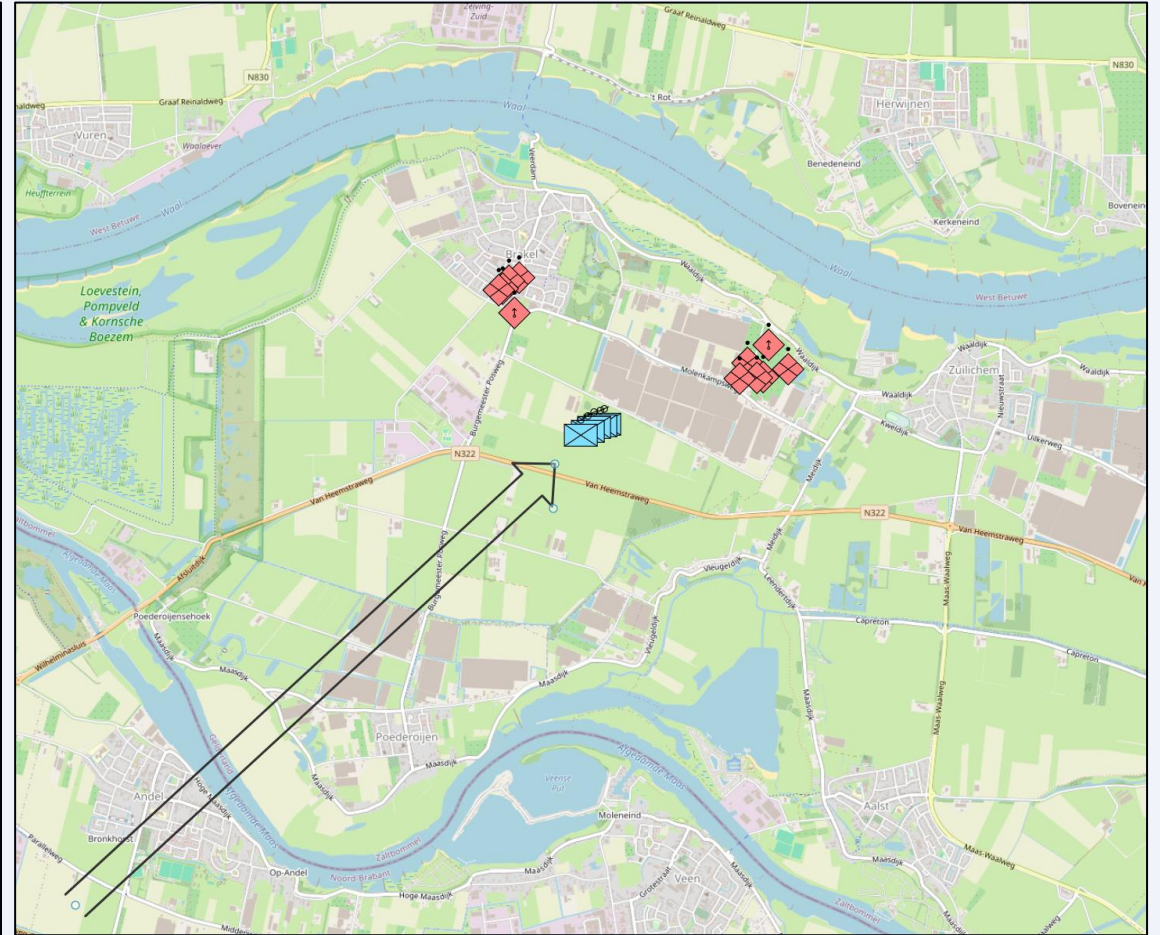
- HLA
- CyberFOM
- APP-6
- APP-11



Cyber awareness bij DHC: CABL



TAK picture (with actual approach)



Ground truth (with easiest approach)

Cyber awareness: RAS

Onderzoek naar de manipulatie van UGV's

- Batterij informatie
- Batterij verbruik
- Beeld manipulatie (ruis)
- Verbindingen
- Zijn standaarden toereikend?
- Bestaande tooling



Cyber in Situational Awareness

Concept development

- Simuleren van sensoren
- Inflight cyber awareness (CEMA)

Waarom in simulatie?

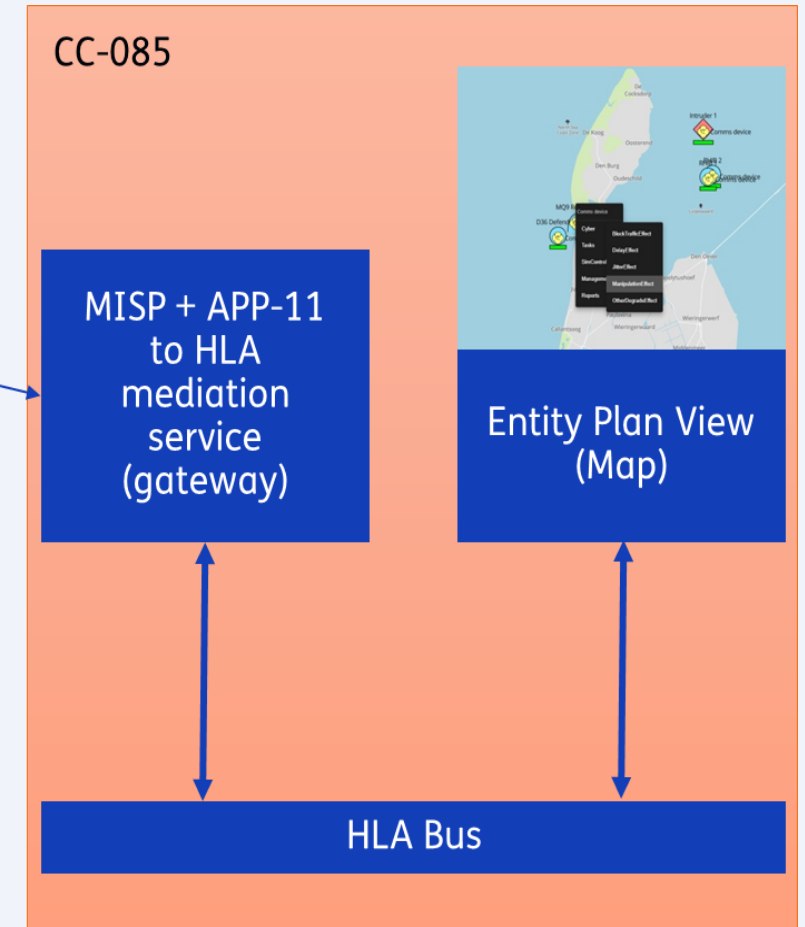
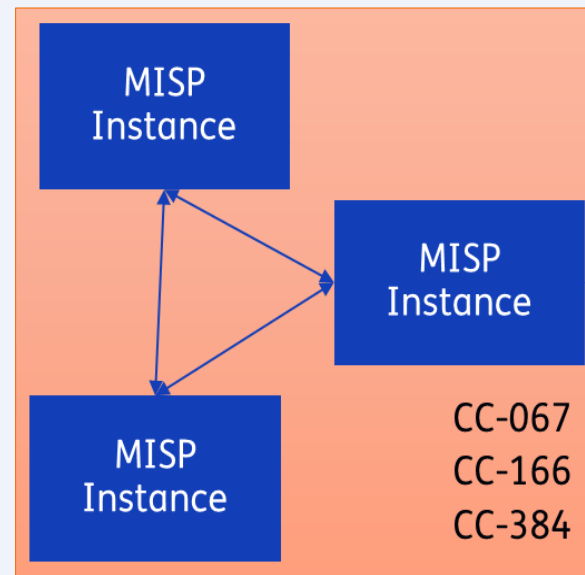
- Kosten
- Resources
- Wetgeving



Tools voor bestaande standaarden

Doel: Onderzoeken van interoperabiliteit met andere cyber systemen en standaarden

- APP-11(NATO)
- APP-6 (NATO)



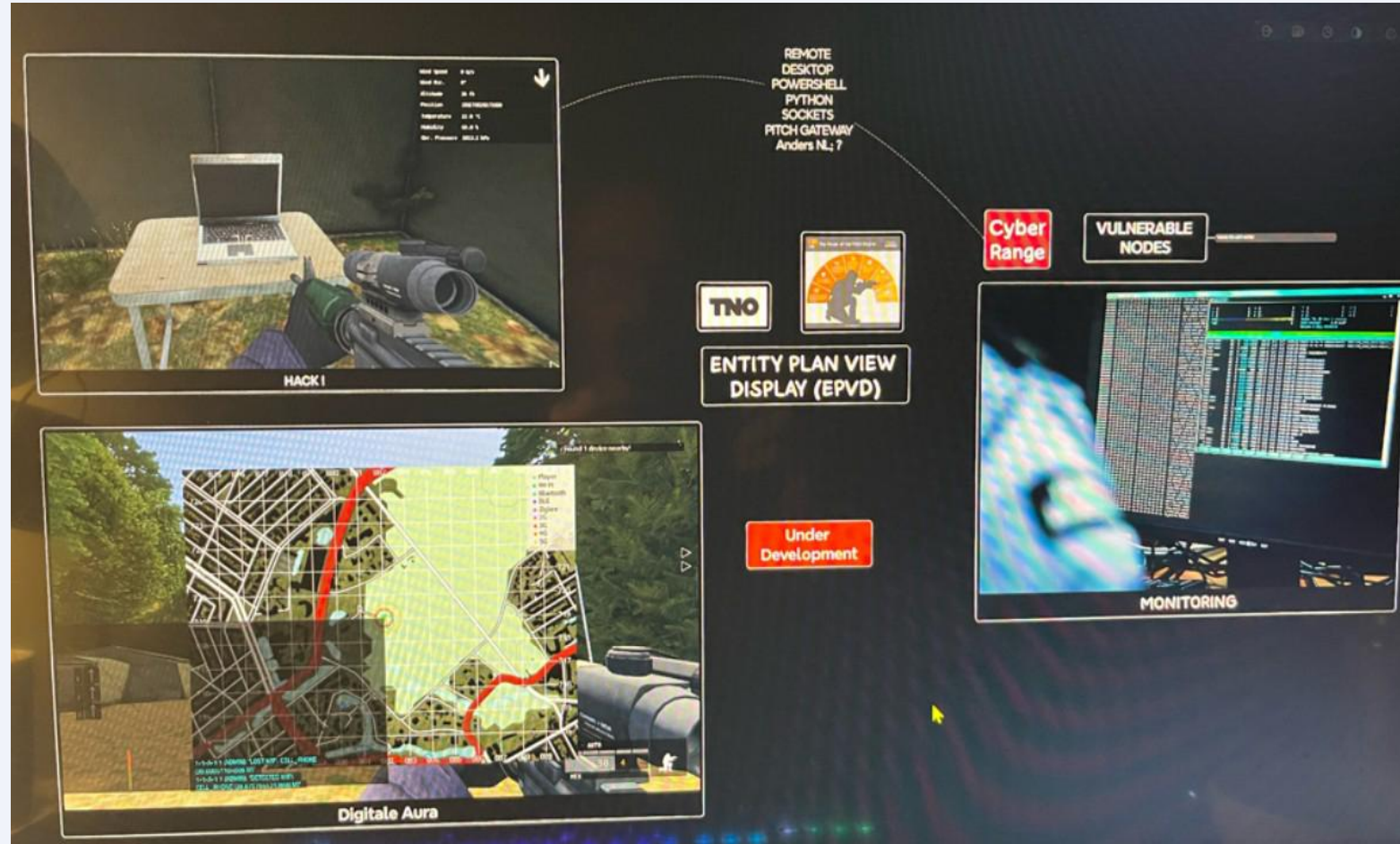
- MISP- malware information sharing platform
- Standard Adatp-5660: “Cyber Security Information Sharing”

SOC scenario training

KMAR - Security operations center

Scenario training voor cyber specialisten

Ontwikkeling van een cyber range koppeling



Evalueren van bestaande tools

Generic Cyber Attacker

Disconnect 

PITCH

▼ CyberEvent

▼ CyberEffect

► Deny

Detect

► Manipulate

▼ CyberAction

▼ CyberAttack

PhishingAttack

▼ ManipulationAttack

KineticManipulationAttack

DataExfiltration

CyberDefend

CyberRecon

CyberAdmin

CyberOrder

CyberAcknowledge

Manipulation-001

6000

Phase

A manipulation attack of 6000 seconds. On GPS location of CH-47.

☒ Request Acknowledgement

Target Identifiers

ID

Actor Identifiers

ID

Source Identifiers

ID

Target Modifiers

GPS

+100

+ - Update

Key	Value
GPS	+100

Manipulation Attack Attributes

Mitre Attack ID

+ -

Send

Clear

pRTI Explorer - CRC

PITCH **pRTI™** **Free** Direct mode CRC listening on all adapters www.pitch.se **HLA EVOLVED**

CRC

General

Federations

VBS

FOM

Federation Info

Diagnostics

Object Instances

Time Graph

Time Table

Synchronization Points

Network Info

Lost federates

GenericCyberAttacker (GenericCyberAttacker)

Declarations

DDM

Known Instances

Trace

Advanced

Interaction Class Subs	Attribute Associations	Regions
Object Class Subs		
Object Class	Attribute	
CyberObject	ObjectID	
CyberObject	Name	
CyberObject	Description	
CyberObject	RelatedObjects	
CyberObject.Network	ObjectID	
CyberObject.Network	Name	
CyberObject.Network	Description	
CyberObject.Network	RelatedObjects	
CyberObject.Network	Protocol	
CyberObject.Network	Mask	
CyberObject.NetworkLink	ObjectID	
CyberObject.NetworkLink	Name	
CyberObject.NetworkLink	Description	
CyberObject.NetworkLink	RelatedObjects	
CyberObject.NetworkLink	DataLinkProtocol	
CyberObject.NetworkLink	Bandwidth	
CyberObject.NetworkLink	Latency	
CyberObject.NetworkLink	Jitter	
CyberObject.NetworkLink	NetworkInterfaces	
CyberObject.NetworkLink.PhysicalNetworkLink	ObjectID	
CyberObject.NetworkLink.PhysicalNetworkLink	Name	
CyberObject.NetworkLink.PhysicalNetworkLink	Description	
CyberObject.NetworkLink.PhysicalNetworkLink	RelatedObjects	
CyberObject.NetworkLink.PhysicalNetworkLink	DataLinkProtocol	
CyberObject.NetworkLink.PhysicalNetworkLink	Bandwidth	
CyberObject.NetworkLink.PhysicalNetworkLink	Latency	
CyberObject.NetworkLink.PhysicalNetworkLink	Jitter	
CyberObject.NetworkLink.PhysicalNetworkLink	NetworkInterfaces	
CyberObject.NetworkLink.PhysicalNetworkLink	PhysicalLayer	
CyberObject.NetworkLink.LogicalNetworkLink	ObjectID	
CyberObject.NetworkLink.LogicalNetworkLink	Name	
CyberObject.NetworkLink.LogicalNetworkLink	Description	
CyberObject.NetworkLink.LogicalNetworkLink	RelatedObjects	
CyberObject.NetworkLink.LogicalNetworkLink	DataLinkProtocol	
CyberObject.NetworkLink.LogicalNetworkLink	Bandwidth	
CyberObject.NetworkLink.LogicalNetworkLink	Latency	
CyberObject.NetworkLink.LogicalNetworkLink	Jitter	
CyberObject.NetworkLink.LogicalNetworkLink	NetworkInterfaces	

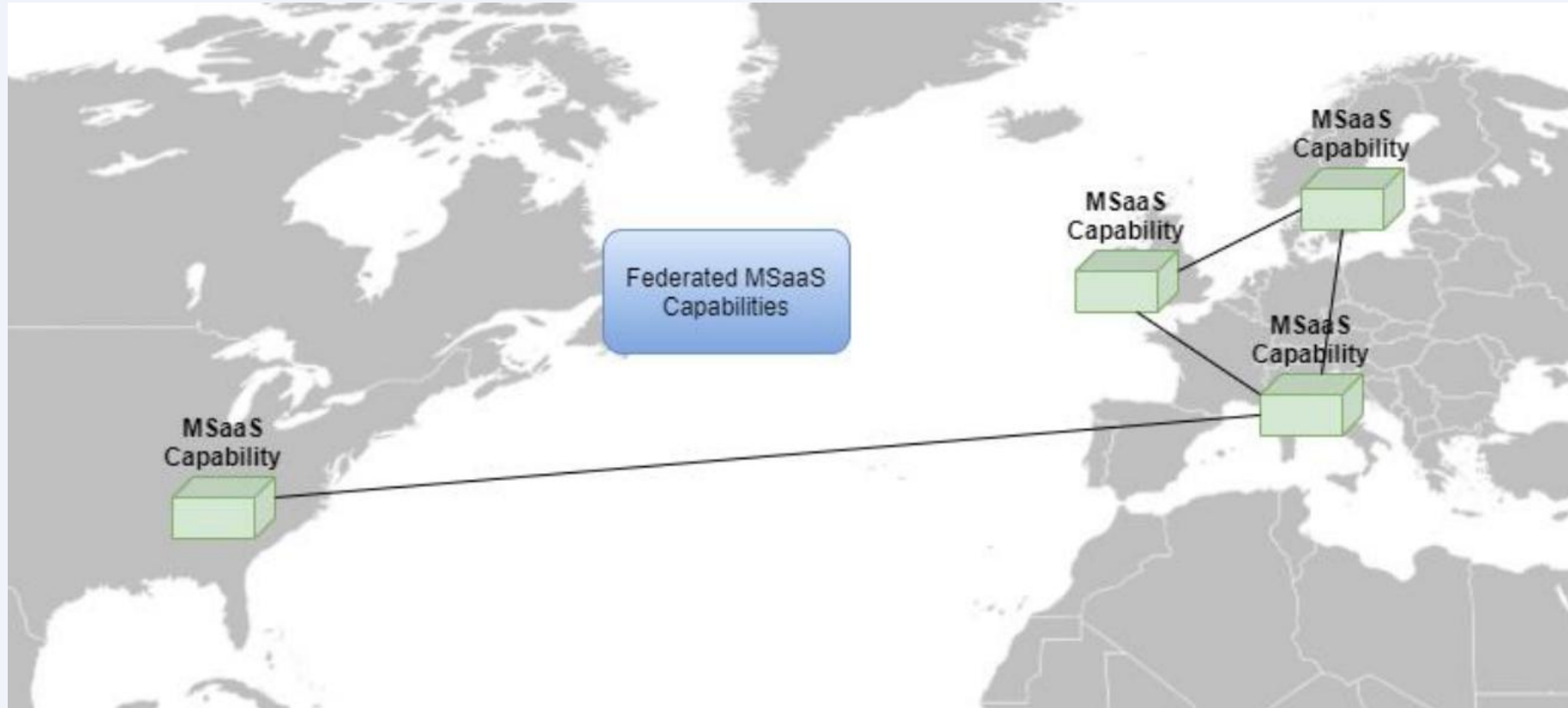
Event Id	Sender	Type	Target Modifiers	Parameters

Herbruikbaarheid

 ais-server TNO AIS Server to stream NMEA-0183 data for simulation... Linux only	 bean-server TNO Bean Server Linux only	 c2sim-gui C2SIM gui for CWIX 2022 Linux only	 c2sim-server C2SIM server for CWIX 2022 Linux only	 orbat-server TNO Orbat Server Linux only	 pitch-booster Connect different sites in a seamless simulation network Linux only	 proto-server TNO Google ProtoBuffer Server Linux only	 sepiatserver TNO SEPIAT Server Linux only
 commander Pitch Commander Linux only	 crc Pitch Central Run-Time Infrastructure Component Linux only	 entity-creator TNO Entity Creator to create simulation entities for NETN... Linux only	 entity-generator VR-Forces NETN Aggregate and Entity Generator Linux only	 smc-agent TNO SMC Agent Linux only	 smc-server TNO SMC Server Linux only	 tilserver Tilserver Linux only	 vessel-traffic-generator VR-Forces Vessel Traffic Generator Linux only
 entity-plan-view-display Entity Plan View Display Linux only	 federation-control TNO Federation Control Linux only	 fft-gateway HLA FFT Gateway and FFT Hub Linux only	 fft-terminal TNO FFT Terminal provides simulated FFT data for... Linux only	 vncwebbrowser VNC Web Browser Linux only	 vtmak-licensemanager MaK License Manager Linux only	 vtmak-rtiexec MAK HLA RTI Executive Linux only	 weblvc-analyser-viewer TNO WebLVC Analyser Viewer Linux only
 filebrowser A Helm chart for the File Browser project Linux only	 geoserver Chart for GeoServer Linux only	 jsonxml-bridge TNO JSONXML Bridge between two HLA federations Linux only	 jsonxml-server TNO JSONXML Server Linux only	 weblvc-server TNO WebLVC Server Linux only	 weblvc-viewer TNO WebLVC Viewer Linux only		
 lox-agent C2SIM LOX agent (execute C2SIM tasks/orders on HLA...) Linux only	 lox-composition LOX Composition Linux only	 lox-control C2SIM LOX control (state synchronisation between C2SIM and...) Linux only	 lox-orbat C2SIM LOX orbat (publish C2SIM initialization...) Linux only				
 lrc-server TNO LRC Server Linux only	 military-symbol Military Symbol Linux only	 nvg-server TNO NVG Server Linux only	 open-cpn OpenCPN Linux only				

MSAAS

Modelling and simulation as a service



MSG-168

Discussie & vragen

Zien wij de connectie met Cyber M&S binnen ons werk?

Zijn er ideeën voor mogelijke CD&E use cases?

Of zien we juist meer mogelijkheden voor cyber awareness?