C2SIM in CWIX

Distributed Development and Testing for Multinational Interoperability

Dr. Mark Pullen

George Mason University C4I & Cyber Center, USA

Lionel Khimeche

DGA, France

Kevin Galvin

Thales, UK

Paper Overview

- Introduction to C2-Simulation Interoperation (C2SIM)
- Complementary SISO and NATO C2SIM Activities
- Distributed Development in NATO C2SIM
- C2SIM Sandbox Cyber Training Capability
- Testing C2SIM in CWIX 2018
- MSG-145 Plans for Expanded Testing of C2SIM
- Conclusions

Introduction to C2-Simulation Interoperation

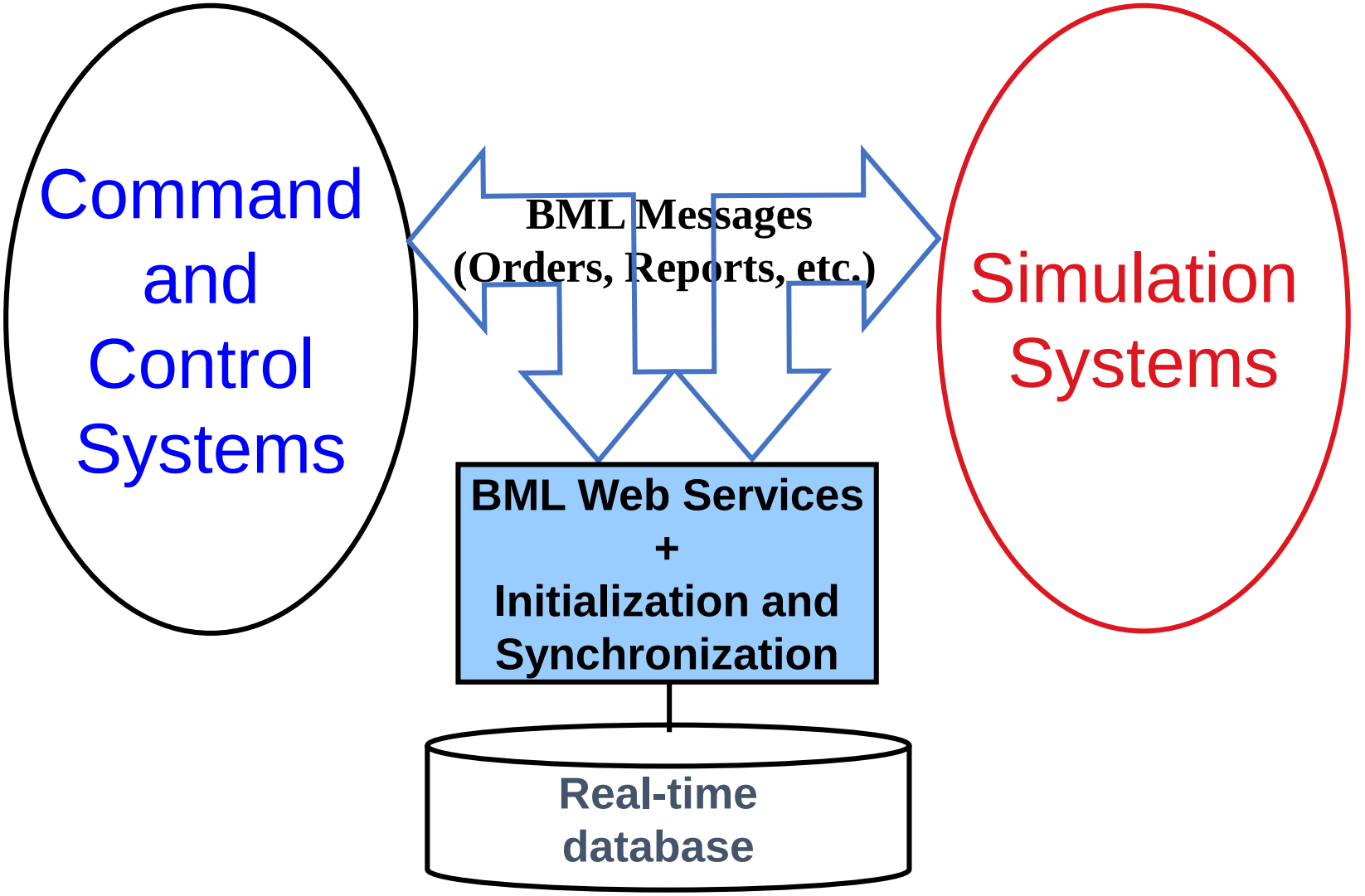
C2SIM Vision

We are working toward a day when the members of a coalition interconnect their networks, command and control (C2) systems, and simulations simply by turning them on and authenticating, in a standards-based environment.

What Does C2SIM Enable

- "Train as you fight"
  - Using operational C2 systems
  - Eliminating human between C2 and simulation systems saves $$$
- Operational planning: COA analysis
- Operational mission rehearsal
- For Service, Joint and Coalition
- France using to support acquisition

C2SIM Basic Architecture



Interdependency of NATO and SISO with regard to C2SIM

NATO MSG depends on SISO for open industry-based standards

SISO depends on NATO Technical Activities to field and validate C2SIM technology

SISO C2SIM Activities

SISO C2SIM Standards

- International, open standards
- Initial versions
  - Military Scenario Definition Language (MSDL) supports initialization
  - Coalition BML (C-BML) provides for exchange of Tasking (orders and requests) and Reporting information
- Unified Version 2 under development as C2SIM
  - Logical Data Model (LDM)
  - Initialization
  - TaskingReporting
  - Extendable to many domains

NATO MSG C2SIM Activities

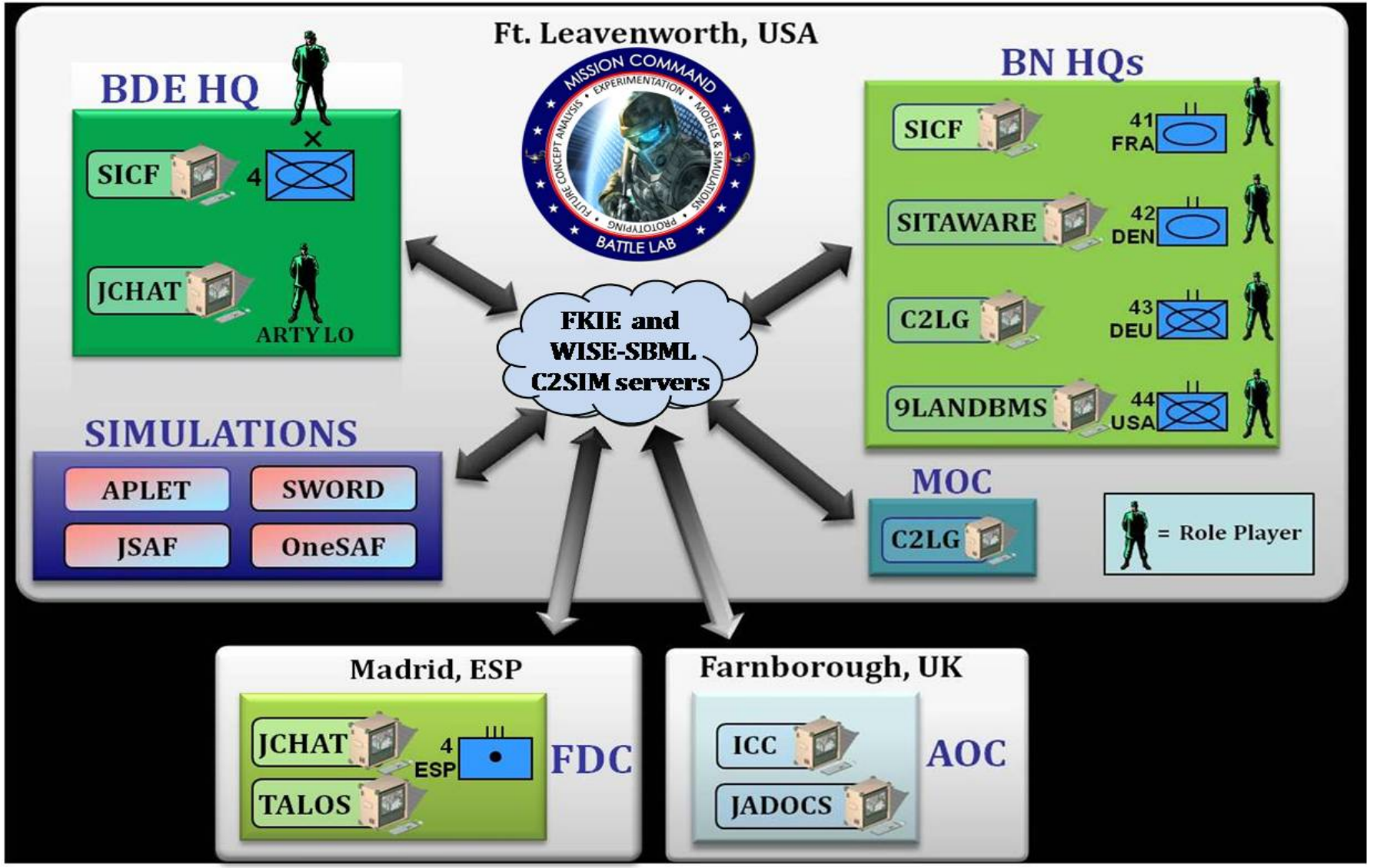
MSG-145 Mission Statement

Assess the C2SIM standard in development and implement extensions to the unified C2SIM Logical Data Model (LDM) for specific functional areas in order to demonstrate its usability to the simulation community and support the definition of a STANAG

MSG-145 Standard Assessment

- **Support the work of the SISO C2SIM PDG in assessing the Draft C2SIM standard, in providing recommendations and in proposing best practices**
  - Review the usability of the core data model
  - Experiment the mechanism of extending the core LDM
  - Check the usefulness of the maneuver warfare extension
  - Review the combination of initialization and tasking/reporting
  - Check the effectiveness and completeness of documentation

C2SIM Example:
MSG-085 Final Demonstration Architecture



How MSG-145 Benefits From CWIX Participation

- Supports our goal of engaging operational NATO military with C2SIM
  - By presenting C2SIM at high visibility in a place where the NATO C2 and Simulation communities come together
- Supports our goal of supporting development of the SISO C2SIM standard
  - By employing the draft standard in a testing environment
- Supports our goal of preparing a STANAG that wraps C2SIM
  - By increasing our understanding of how C2SIM can be used

Distributed Development in NATO MSG C2SIM

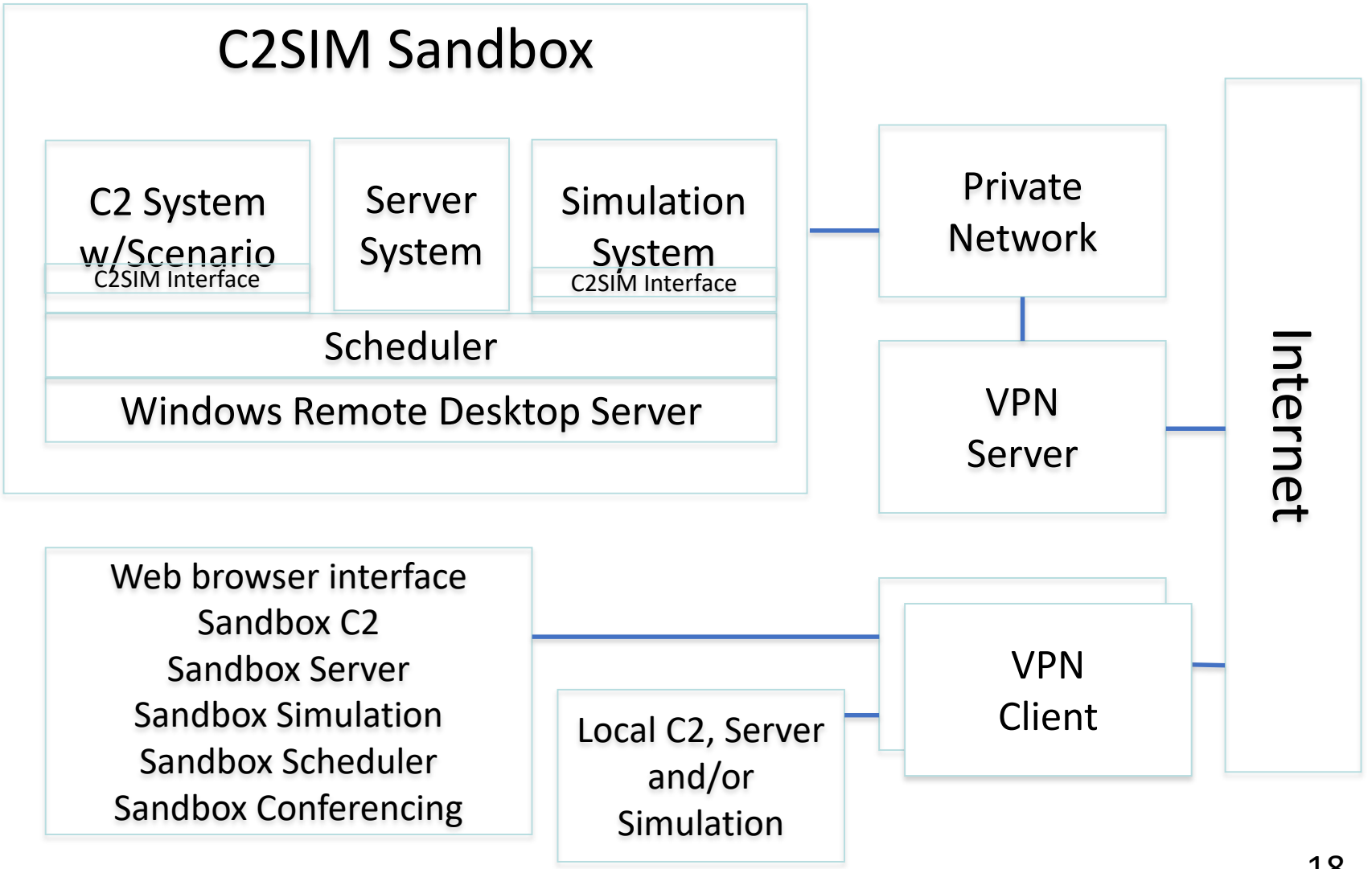
Why Distributed Development Support

- MSG support teams are geographically distributed
  - Travel to bring them together is costly
  - Sometimes process takes longer than expected, as happened in MSG-048
- Open Internet is attractive for communication but unstable/insecure due to hackers
- Secure, established facilities operating 24x7 needed to reduce setup time for debugging/testing/ demonstration/experimentation

C2SIM Sandbox Concept

- VPN-based collaborative environment
  - Credentials for all MSG-145 members
- Application GUIs available via Web browser
- Available to run on-demand 24x7
  - GMU Java-based reference implementation schema-translating server
  - GMU BML C2 GUI
  - MÄK VRForces with C2SIM interface
- Web-based scheduler (one-hour slots)
  - Includes ability to provide application parameters
- Web-based conferencing
- Financial support from NATO CSO

C2SIM Sandbox Architecture



Ways to Employ the Sandbox

- C2SIM demonstrations
  - Schemata: IBML09, IBML09+, CBML Light, C2SIM Core
  - C2SIM Maneuver Warfare when available
  - Generic scenario provided (others if contributed)
- C2SIM testing
  - Test C2 with Sandbox Server and Simulation
  - Test Server with Sandbox C2 and Simulation
  - Test Simulation with Sandbox C2 and Server
  - Test C2-Simulation Coalitions with the Server
  - Distributed configurations of all sorts
- Distributed system of Sandboxes
- C2SIM validation with SISO
- C2SIM-based exercises (server performance limits scope)

Testing C2SIM in CWIX 2018

C2SIM CWIX 2018 Scenario

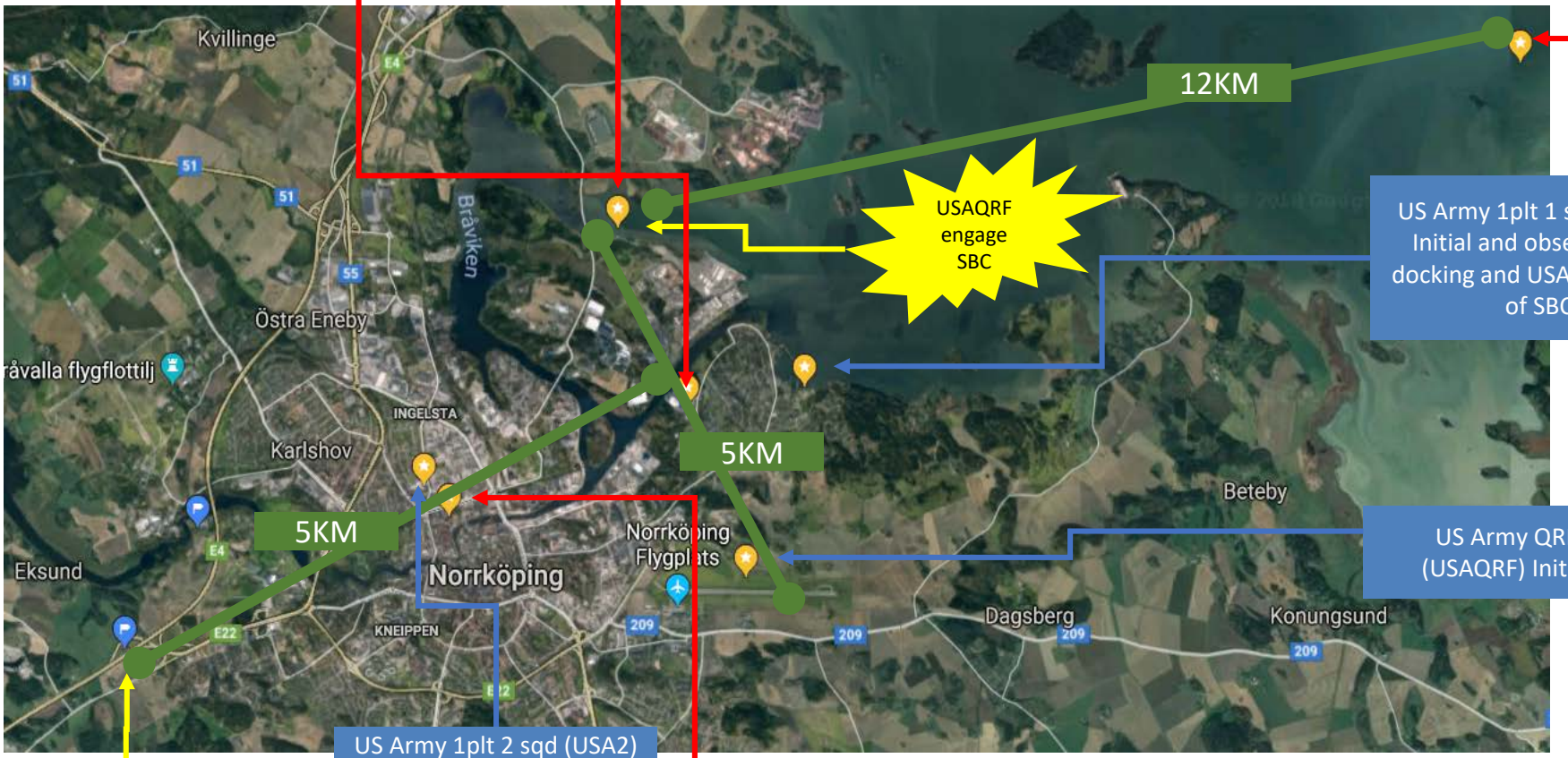
To motivate the activities tested, military officer students at USA Naval Postgraduate School developed a scenario

- The CWIX test is about information interoperability
  - The scenario helps make sure we're testing the right transactions
- Asymmetric peacekeeping operation in Bogaland
- OPFOR:
  - five terrorist cells
  - modified commercial vehicles
  - weapons transport boat
- Peacekeepers:
  - One infantry platoon
  - Helicopter Quick Reaction Force
  - Surveillance UAS
  - Attack UAS

CWIX 2018 Scenario: H0 to H1

- H0 to H1
  - Blue forces are primarily conducting reconnaissance while Red forces are continuing to conduct logistics operations in the vicinity of Norrköping and Linköping
  - UK Reconnaissance UAS (UKUAS1) detects two small boats (SBC) moving weapons and bomb-making materials via Bråviken Bay to Norrköping
  - UK Reconnaissance UAS (UKUAS2) detects a convoy moving weapons (NC1) to Linköping via local streets to E22 then to Highway E4
  - US Ground Forces (3) (USA3) from Linköping patrolling northeast of the city detect a small safe house along the Highway E4. There seems to be a squad team sized element (SHC) on guard
  - QRF is launched from Norrköping Airfield to interdict a small boat delivery of weapons at the inlet of Motala Ström River. US Ground Forces (1) (USA1) observes their activity

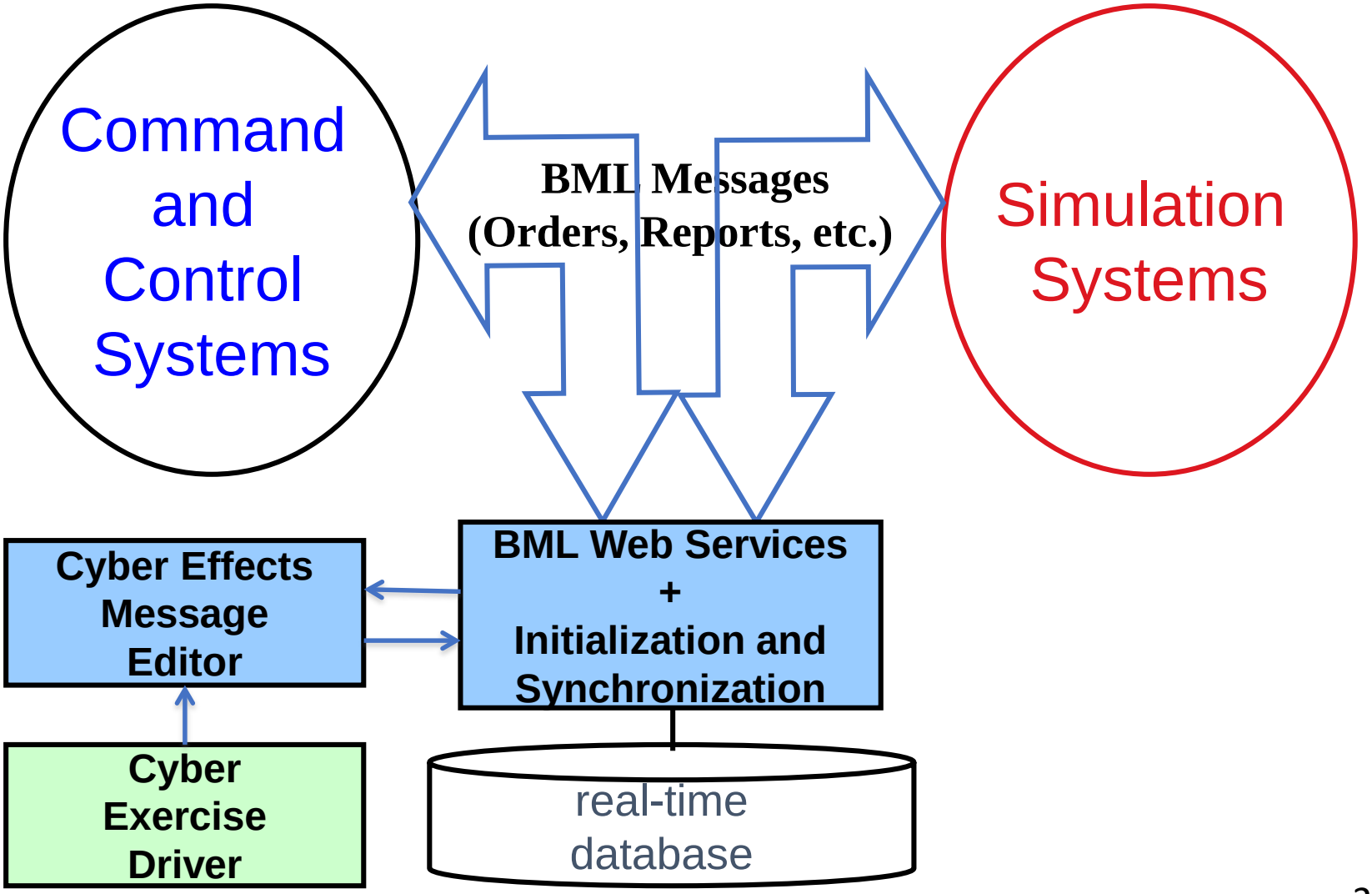
CWIX 2018 MSG-145 C2SIM Scenario Locations



Importance of Training in Cyber-Active Environments

- Two kinds of cybersecurity training:
  - Cyber specialists defending from (attacking?) adversaries
  - Operational military who may have to function under cyber-active conditions
- Second was tested in CWIX 2018 and is critical
  - Forces must not be crippled by cyber attack!
- Concern is for cyber + electronic warfare (CEMA) because impact on operations can be similar
- Actually compromising command and control (C2) would be very disruptive to training exercises
- Modifying the systems so they appear to be compromised is possible but expensive/time-consuming

C2SIM Cyber Effects in Operational Training
Expanded C2SIM Architecture

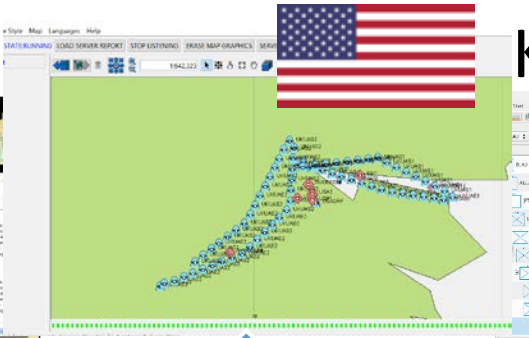


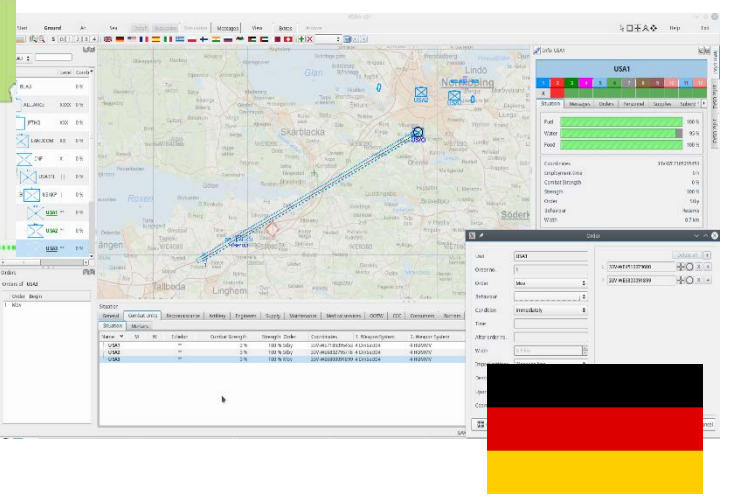
CWIX 2018 C2SIM Configuration

- One C2IS
  - Norway NORCCIS/SWAP
- Three simulations:
  - Germany KORA air UAV attack; ground force
  - US VR-Forces
  - UK JSAF air UAV recon
- Supporting:
  - US BMLC2GUI editor (receive, visualize and push XML)
  - US C2SIM Reference Implementation Server
  - Scenario assisted by US Naval Postgrad School
    - Asymmetric operation with UAVs

NORCCIS

KORA

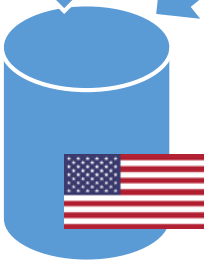




ORBAT

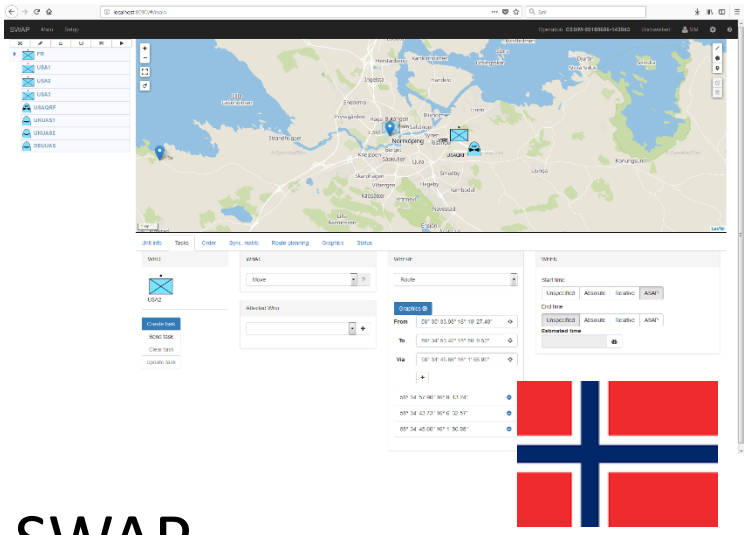
Tactical graphics

NFFI

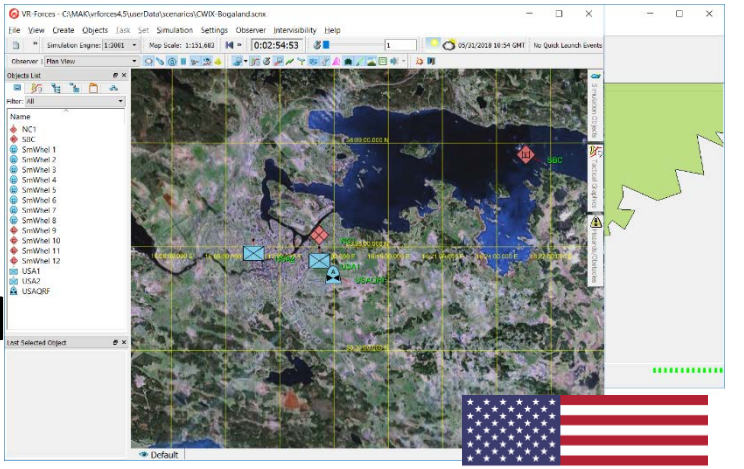


C2SIM

draft standard

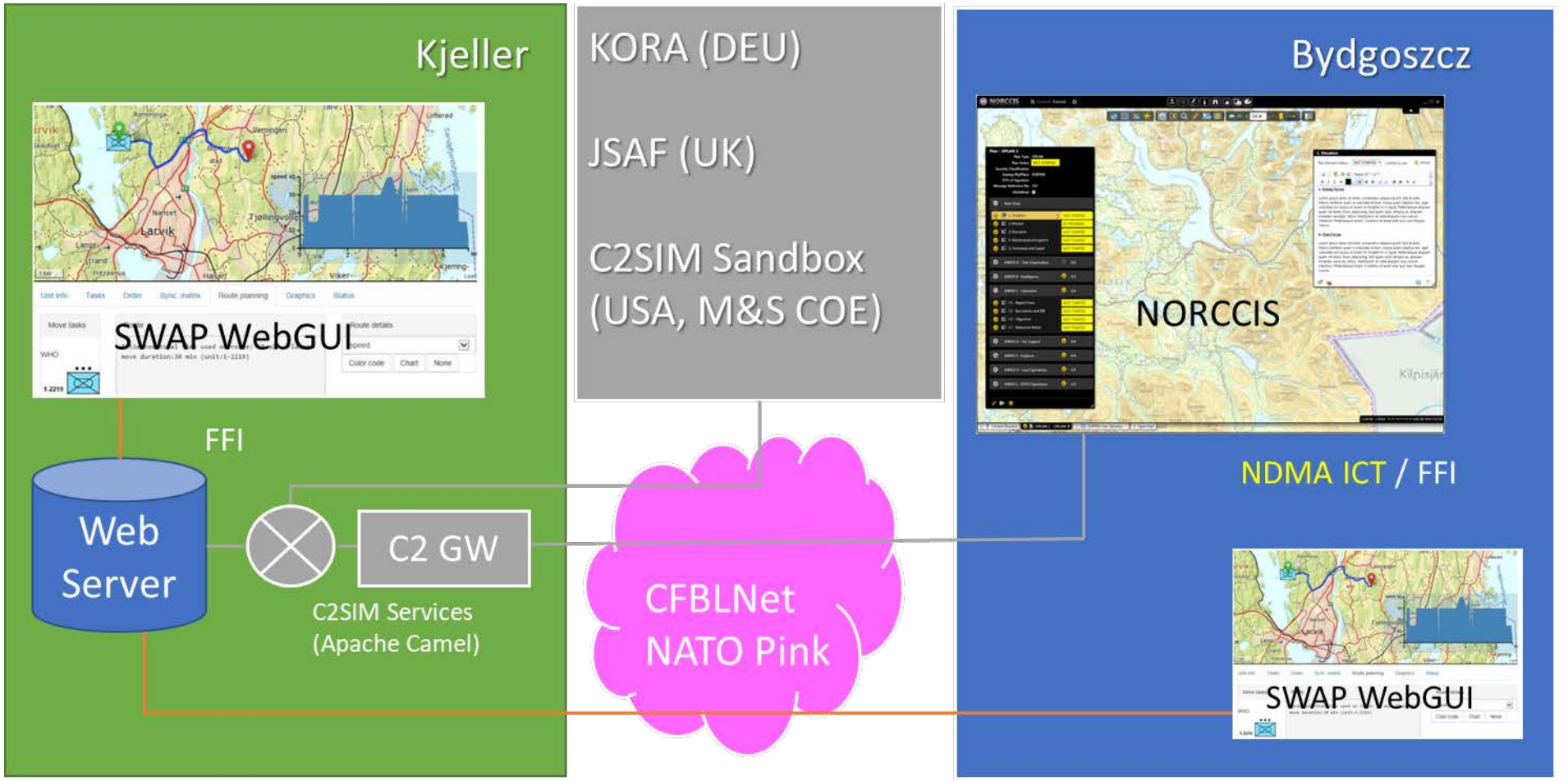


SWAP



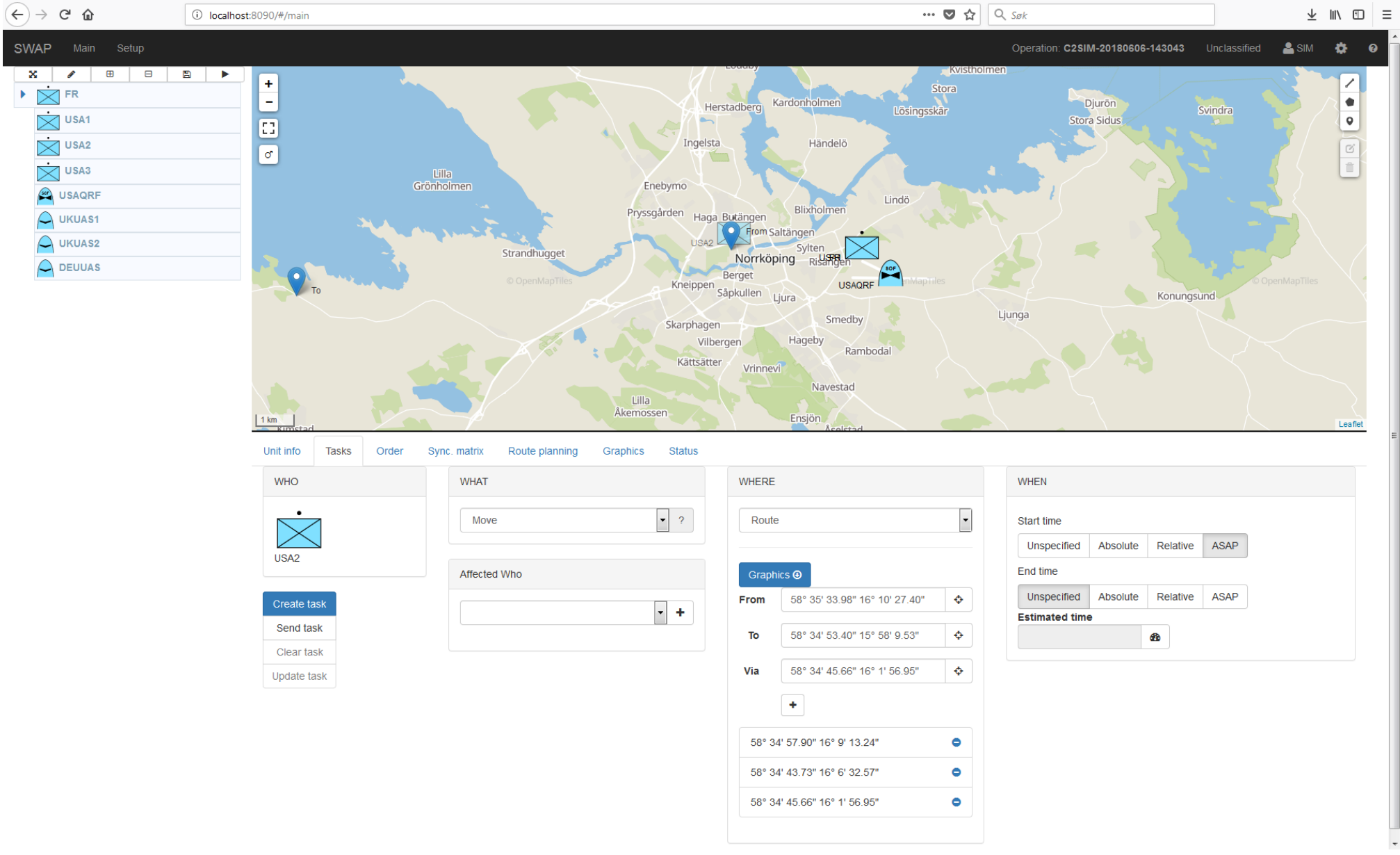
VR-FORCES

MSG-145 Web-Enabled C2SIM Capability Demonstration

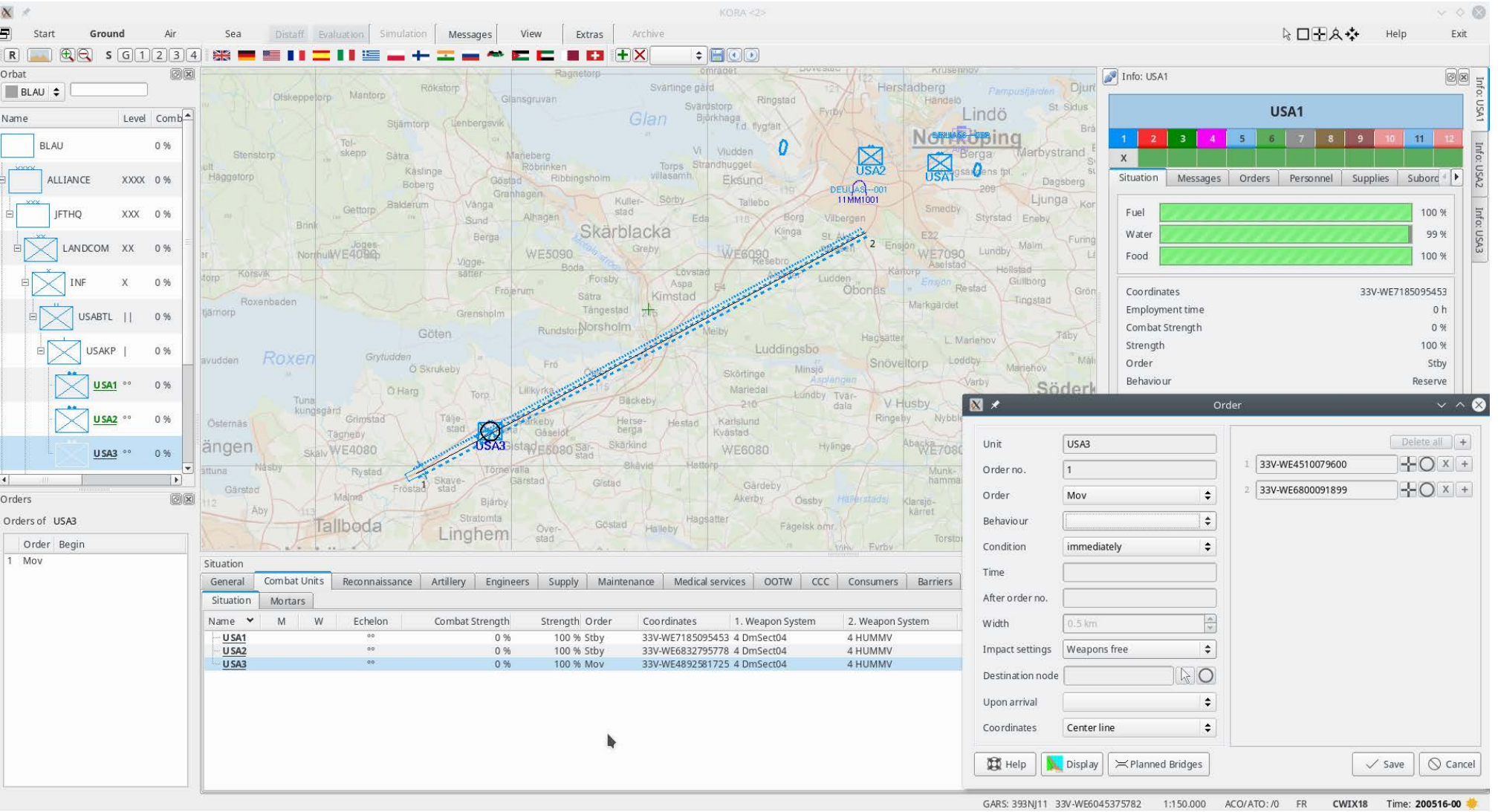


- Develop Task Organization and Tactical Graphics using NORCCIS
- Develop executable Order using FFI SWAP WebGUI
- Simulate Order with GMU C2SIM Sandbox

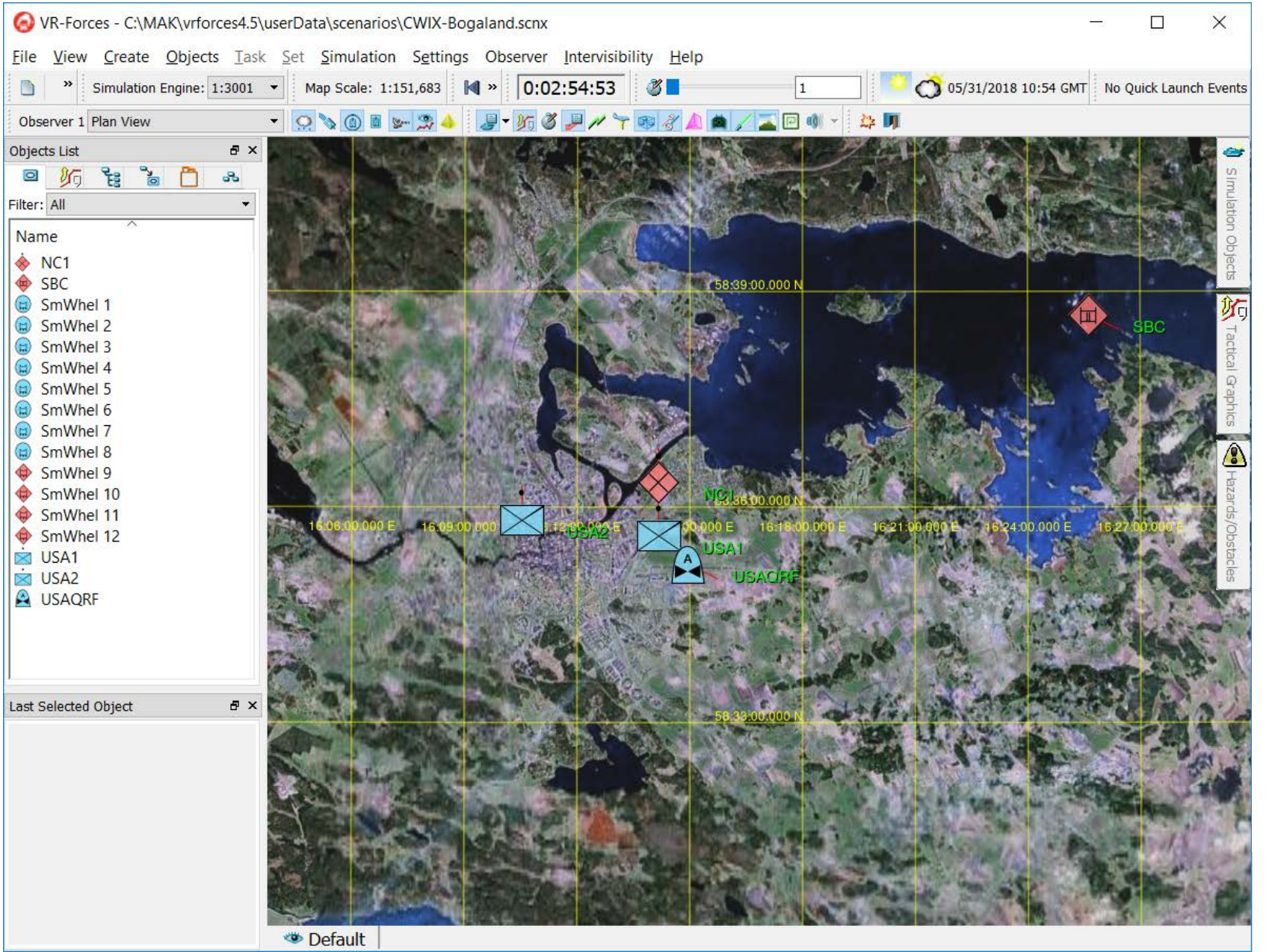
SWAP Web-based C2 for NORCCIS



KORA German Simulation

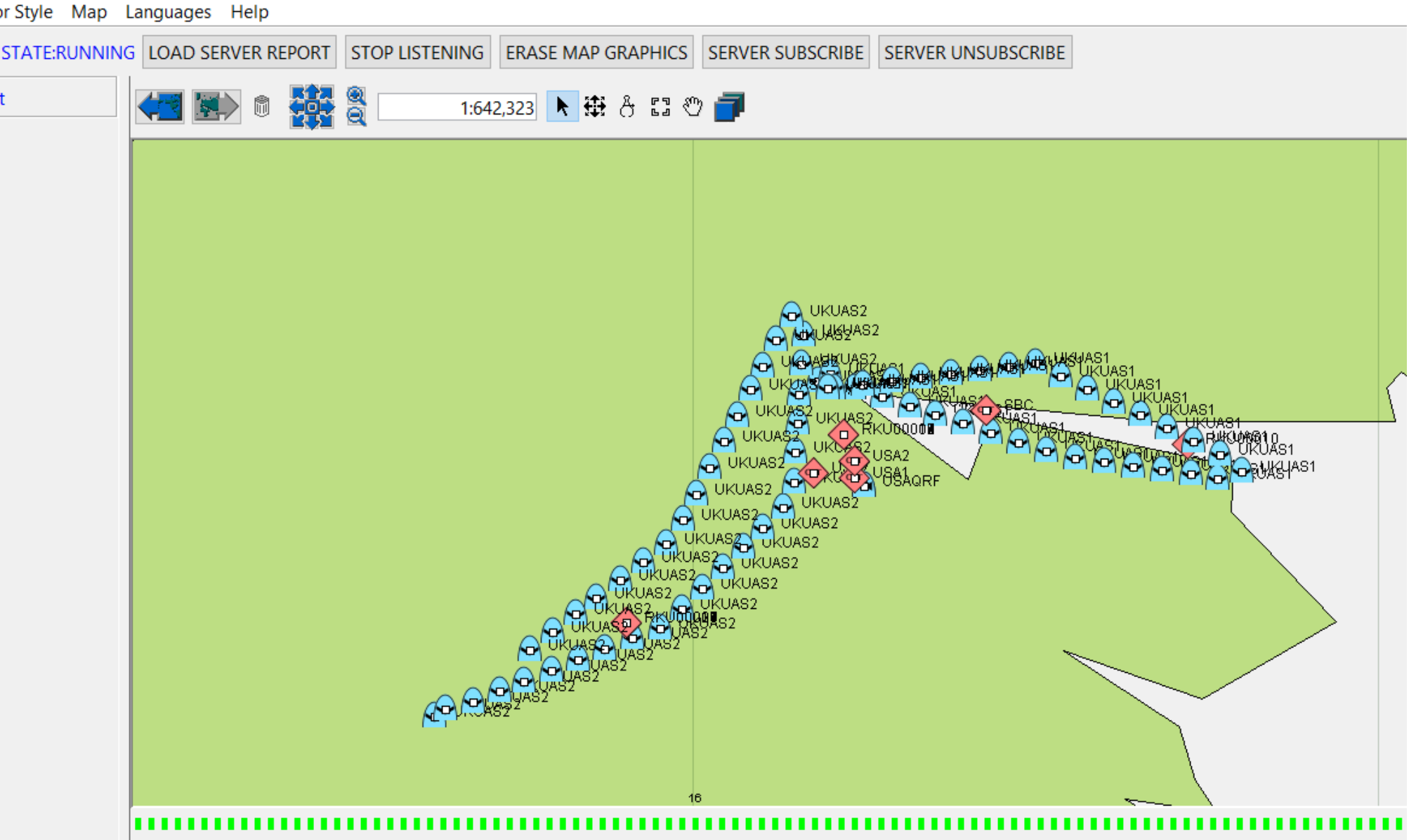


VR-Forces Commercial Military Simulation



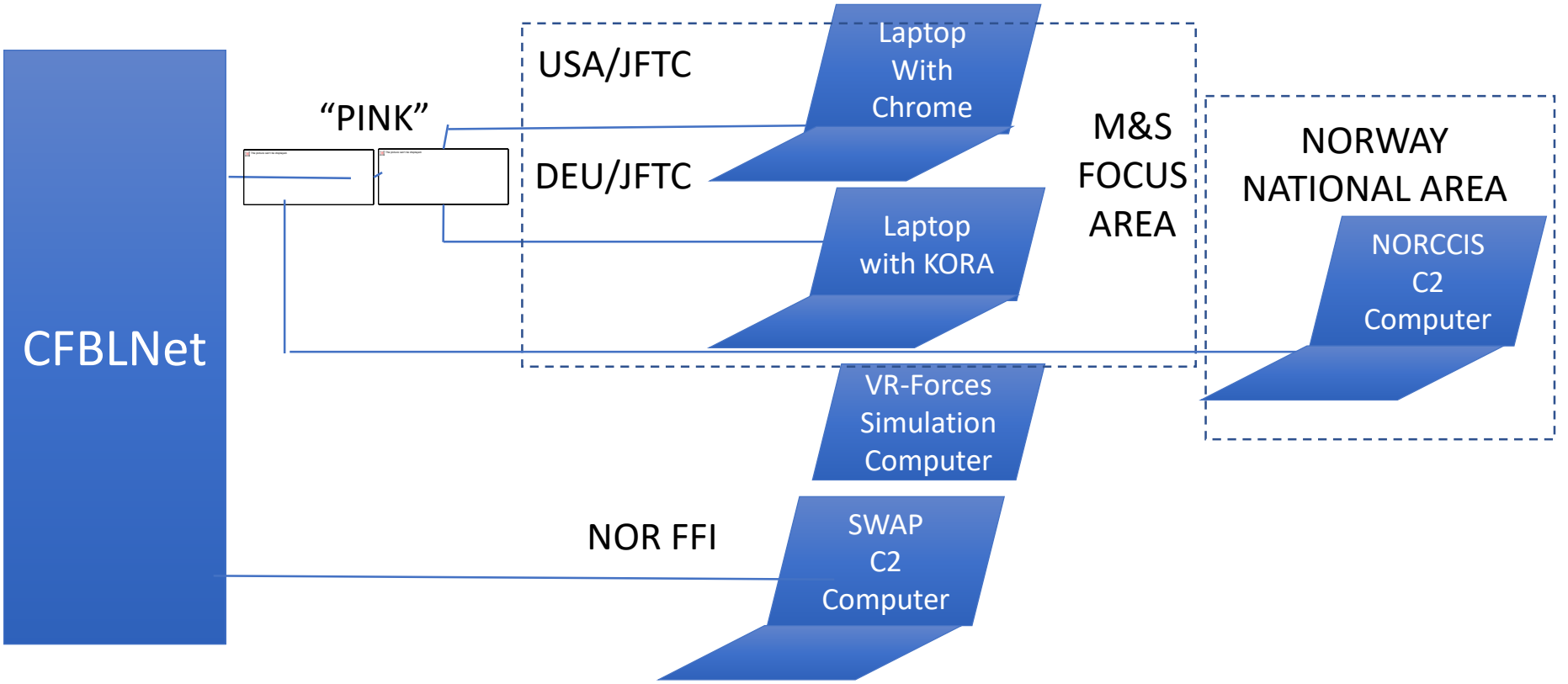
GMU Open Source BMLC2GUI Editor

showing JSAF UAS recon patterns



CWIX 2018 MSG-145 Network Diagram

as executed



Testing Results

- Phase 0 Confirm network connections: (Major change from testing plan: three of the four CFBLNet sites were not available)
  - However we had fallback copies of VRForces and C2SIM Server
  - And a recorded trace of JSAF UAS reports (Blue and Red)
  - So we were able to carry out most planned testing
- Phase 1 Confirm server compatibility:
  - Success with all client-server connections except missing JSAF
- Phase 2 Test C2SIM interoperation among all systems:
  - Success with NORCCIS sending orders to KORA and VR-Forces and receiving orders
  - Use recorded reports from JSAF to provide background traffic
- Phase 3 All systems engaged simultaneously with cyber:
  - Successful with air, then ground; when testing ALL, found and fixed a bug
  - Cyber worked as expected

Conclusions

MSG-145 Planning for CWIX 2019

- CWIX 2018 testing has some limitations
  - Limited operational scope
  - Only one operational military C2IS
  - Simulations not interoperating on data side (only C2 side)
- For CWIX 2019 we would like to
  - Increase scope of scenario and resulting C2 data flows
  - Have at least two operational military C2IS
  - Simulation data interoperating over DIS or HLA
- Also would like to partner with other advanced C2 and simulation activities
  - Modeling & Simulation as a Service (MSaaS)
  - NATO Federated Mission Network planning (FMN)

QUESTIONS