Live, Virtual, Constructive HybrId CYBer warfarE Range (HI-CYBER)

A M&S architecture and tools for security issues analysis countering Hybrid Cyber warfare threats

LTC (ITA Army) Marco BIAGINI
NATO M&S CoE
mscoe.cd01@smd.difesa.it

LTC (ITA Army) Walter DAVID
NATO M&S COE
mscoe.cd08@smd.difesa.it

LTC (ITA Army) Ferdinando BATTIATI
Italian Army School of Transmissions and Informatics (SCUTI)
ferdinando.battiati@esercito.difesa.it

Agatino MURSIA
Engineering Head of Innovation
Leonardo – Land & Naval Defence Electronics Division
agatino.mursia@leonardocompany.com

Lucio GANGA
Engineering Innovation
Leonardo – Land & Naval Defence Electronics Division
lucio.ganga@leonardocompany.com

NATO MSG-143 Symposium, Bucharest, Romania, 20-21 October 2016
Presenters: LTC Walter David, Mr. Agatino Mursia

Agenda

- Non-linear and Hybrid warfare
- Countering Cyber threats in a Hybrid warfare environment
- Cyber Security Simulation Environment (CSSE)
- Live Virtual Constructive (LVC) Hybrid Cyber warfare Range (HI-CYBER)
- The HI-CYBER Concept
- Cyber Attack Simulator and other components
- Use Case
- Conclusions

Introduction

You might not be interested in hybrid warfare, but hybrid threats are definitely interested in you *(A. Butenschön)*

- **Hybrid warfare** not new but… recent simultaneous, evolving threats of Hybrid Warfare (HW) in all physical environments and the information space.
- Target civilian and military decision making processes and human/social behaviour to achieve (geo) strategic goals.
- Protection of Communication Networks and related information flow is crucial.
- **Paper** proposes a **Live Virtual Constructive (LVC) Hybrid Cyber warfare Range (HI-CYBER)** as simulation-based experimentation environment for Hybrid threats. scenarios

Hybrid warfare

Cyber attacks

Information warfare/ propaganda

Special Forces

Regular Military Forces

MIX of *civilian and (overt and covert) military (full Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal DIMEFIL spectrum) to achieve (geo)strategic goals*

Non-linear War as part of a process, not necessarily its most important part *(V. Surkov)*

Asymmetric, Information warfare, Cyber warfare *target military and civilian comms, networks, Information systems and decision making processes and human/social behaviour*

Economic warfare

Irregular Forces

Terrorism

Support of Social unrest

Diplomacy

The use of military forces

Traditional forms and methods

-initiation of military operations ***after strategic deployment***

-***frontal clash of large groupings of line-units***, the basis of which consists of ground troops

-the destruction of personnel and weaponry, and the ***consequent possession of lines*** and areas with the goal of the seizure of territories

-***destruction of the enemy***, destruction of the economic potential and possession of his territories

-the conduct of combat operations on the ground, in the air and at sea

-the command-and-control of groupings of line units (forces) ***within a framework of a strictly organized hierarchical structure*** of command-and-control agencies

The use of political, diplomatic, economic and other nonmilitary measures in combination with the use of military forces

New forms and methods

-***initiations of military operations*** by groupings of line-units (forces) in peacetime

-***highly maneuverable, noncontact*** combat operations of inter-branch groupings of line-units

-reduction of the military-economic potential of the state by the ***destruction of critically important facilities*** of his military and civilian infrastructure in a short time

-the ***mass use of high-precision weaponry***, the large-scale use of ***special operations forces***, as well as ***robotic systems and weapons based on new physical principles*** and the participation of a ***civil-military component*** in combat operations

-***simultaneous effects*** on line-units and enemy facilities throughout the entire depth of his territories

-warfare simultaneously ***in all physical environments and the information space***

-the use of asymmetric and indirect operations

-command-and-control of forces and assets ***in a unified information space***

Graphic from Gen. Valery Gerasimov article in Voyenno-Promyshlennyy Kurier, 26 February 2013, translated by Charles Bartles.

Countering Cyber threats in Hybrid warfare

Cyberspace as 5th domain of Operation

- Coordinated computer-based Cyber-attacks by state/non-state actors.
- Cyber ad Information are dual (civil and military) issues.
- Cyber-attacks disrupt/deny IT Infrastructures and/or access to Information.
- Corrupted, misleading information affect C2 and decision making processes (impact of trust to integrity and availability on OODA Cycle).

Proposed Solution:

- Countering Cyber threats in a Hybrid environment by extending the Hybrid warfare Concept Development under NATO MSG ET-043.
- Definition of a **L V C Architectural Framework** to investigate, evaluate the comms and network security issues under Cyber attack in a Hybrid warfare environment.

HI-CYBER

Cyber Security Simulation Environment (CSSE)

- It is a project carried out under the Italian National Military Research Plan (PNRM).
- It arises from the need to evaluate, through the use of advanced simulation tools and architectures, scenarios related to communications networks (tactical or infrastructural) of military units facing cyber threats.

CSSE Overview

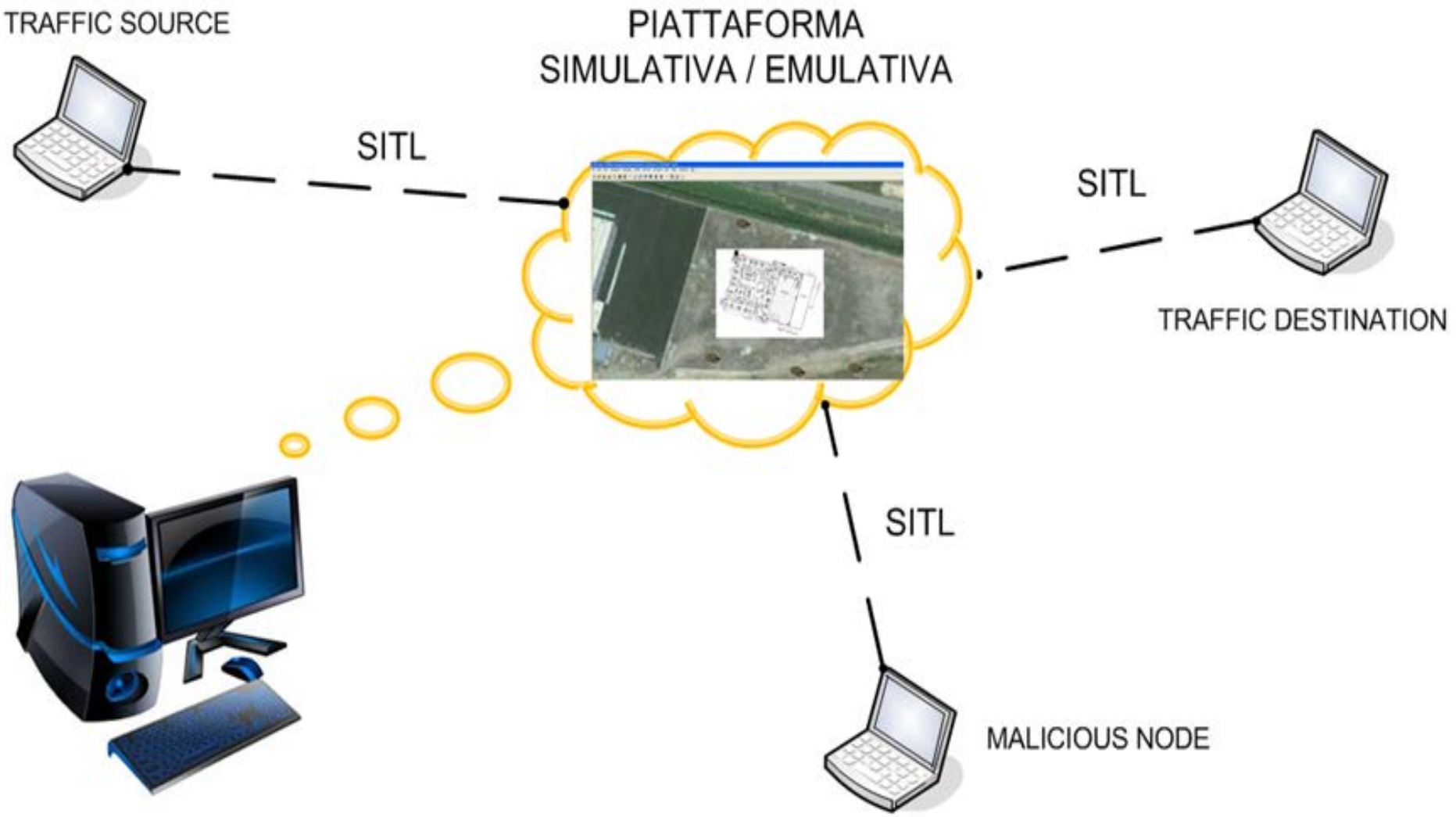
CSSE has used, as references, the outcomes of NATO working groups in the international arena such as:

- NATO SAS-065 (NATO C2 Maturity Model)
- SAS-085(C2 Agility)
- MSG-117 (M&S in support of Cyber Defence)

CSSE Objectives

- Analyse the state of art in the fields of Modelling and Simulation and Cyber Security and put them in synergy with a detailed focus on military networks and cyber threats;
- Define and describe operational scenarios, making also reference to the outcome of NATO SAS-065 and NATO SAS-085 in terms of possible scenarios, in which operate military tactical networks and also civil NGO networks subjected to cyber-attacks;
- Define and develop ad-hoc models and a simulation architecture that will allow for building a test bed environment (demonstrator) in which attackers and defenders can exercise the scenarios, cyber threats and related countermeasures previously identified without disturbing and affecting the real operational network;
- Evaluate, on the demonstrator, different situations, building a repository of reference scenarios to be used for cyber operators training;
- Disseminate the results obtained from the campaign of experiments

Live-Constructive CSSE Architecture



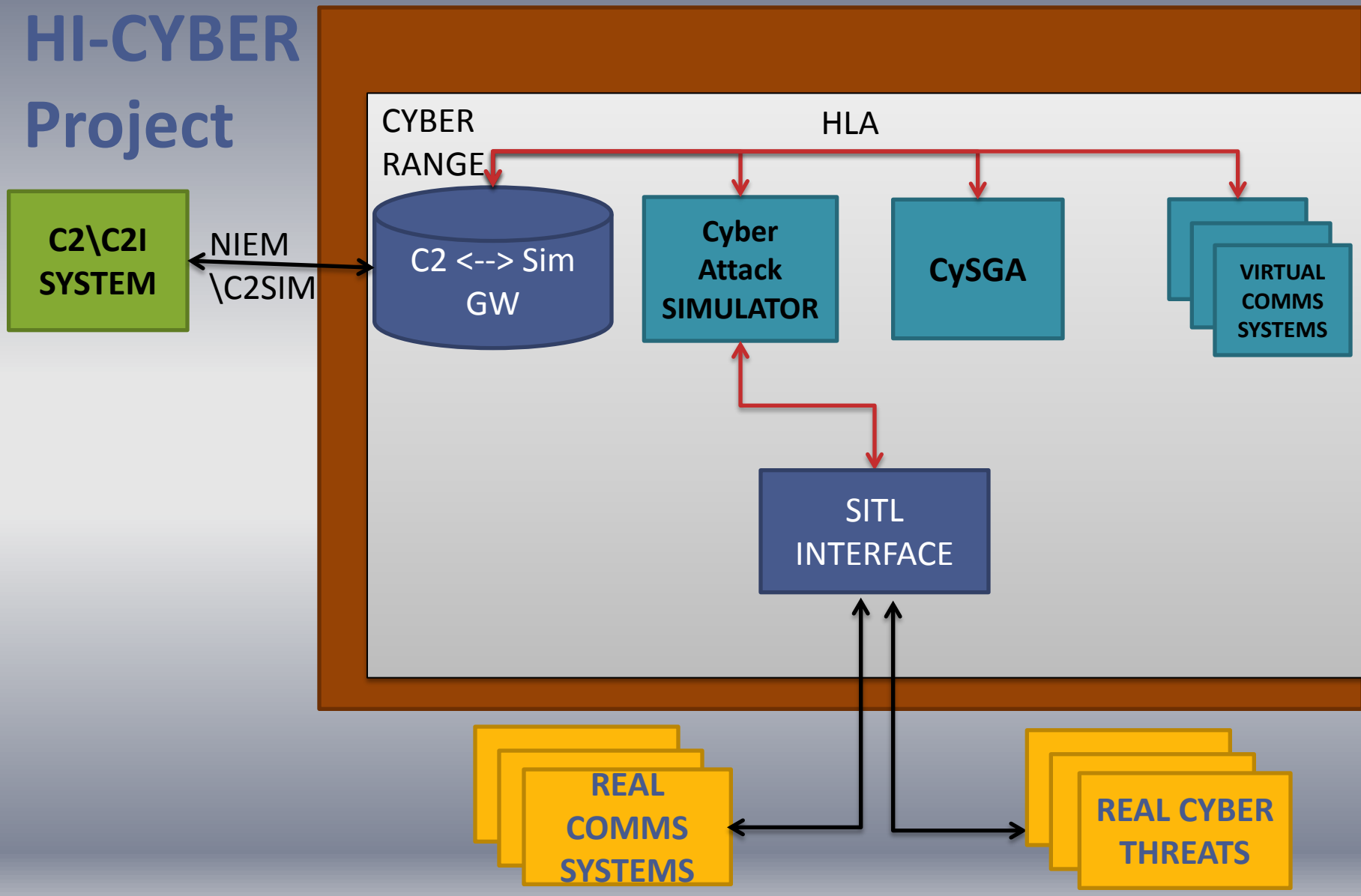
The HI-CYBER Concept

- The LVC (Live Virtual Constructive) HI-CYBER concept has been developed as an emerging one concept to support countering Hybrid Cyber-warfare extending the Hybrid Warfare Concept Development activities under the NATO MSG ET-043.

- HI-CYBER originates from the implementation and customization of National (Italian) Military Research Program (PNRM) CSSE that, for the characteristics and functionalities described before, represents a good starting point for the creation of a more complex demonstrator where the Cyber threats are one of the many dimensions within the Hybrid Warfare.

- HI-CYBER environment is composed by: The **Cyber Attack Simulator**, the **Hybrid Warfare Scenario Generator and Animator (HW-SGA)**, **C2 systems**, **Live, Virtual and Constructive tools**, exploiting heterogeneous technologies, through Systems in the loop (SITL), High Level Architecture (HLA) Run-Time Infrastructure (RTI), gateways between different communication protocols.

HI-CYBER Project



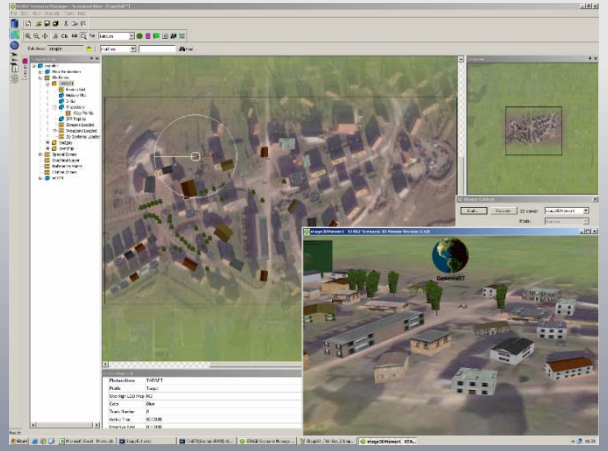
HI-CYBER Features

- Communication and Networking architectures Modelling and Simulation.
- Real Cyber Attack and countermeasures mixed with simulated ones.
- Real Communication Systems to simulated Environment interaction (Live and Virtual).
- Federated and integrated with the C2 Systems.

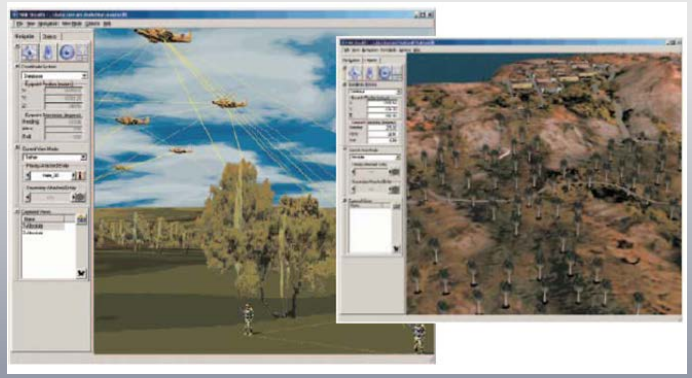
HI-CYBER Components

Virtual Communication Systems

Real Communication Systems



Scenario Generator

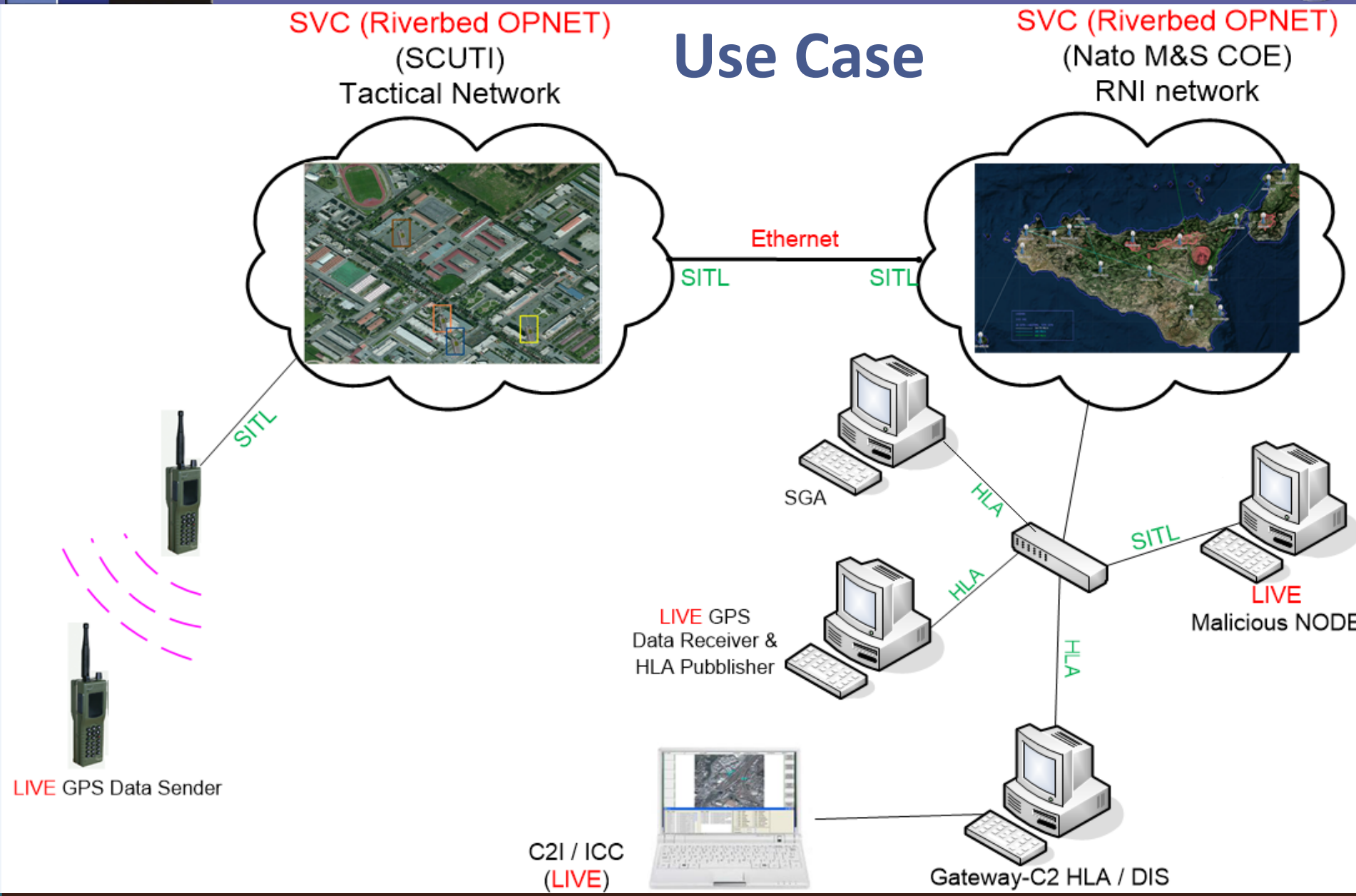


Communication Network Simulator

Cyber Attack Simulator

- Plays a relevant role in the simulation architecture oriented to test cyber effect
- Offer a complete overall vision of all the concurrent factors
- Performances analysis:
  - ✓Effects of physical layer attacks
  - ✓Effects of network protocol attacks
  - ✓Analysis of simulated countermeasures on real cyber threats
  - ✓Analysis of simulated attacks on real traffic

Use Case


SVC (Riverbed OPNET)
(SCUTI)
Tactical Network
SVC (Riverbed OPNET)
(Nato M&S COE)
RNI network
Ethernet
SITL
SITL
SITL
SGA
HLA
SITL
LIVE
Malicious NODE
LIVE GPS
Data Receiver &
HLA Pubblisher
HLA
HLA
LIVE GPS Data Sender
C2I / ICC
(LIVE)
Gateway-C2 HLA / DIS

Conclusions

- The HI-CYBER Concept considered Hybrid threats simulated in a Constructive simulation and executed in combination with simulated/real Cyber attacks within a LVC federation.
- Further development is required to properly run the experimentation phase to support the proof of concept.
- Hybrid threats ad-hoc scenarios and tactical vignettes should be developed within the Virtual and Constructive simulation.
- Possible investigation on Hybrid warfare behavior models, affecting humans and Communication and Network systems in relationship with cyber and other hybrid threats.

Questions & Answers