Simulation Team

Simulation Models for Hybrid Warfare & Population Simulation

DIME
Università
di Genova

A.G. Bruzzone
M. Massei

Simulation Team
www.simulationteam.com

R. Di Matteo
G.L. Maglione

F. Longo

P. Di Bella

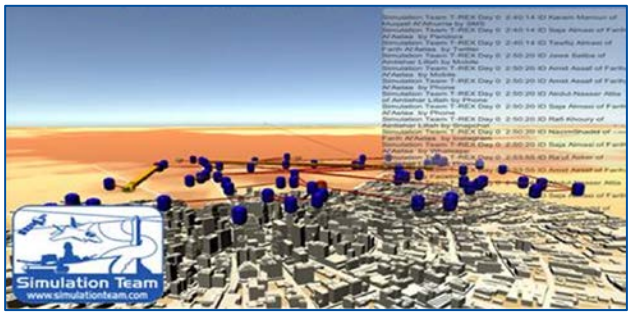
FEYZİYE MEKTEPLERİ VAKFI
IŞIK ÜNİVERSİTESİ

E. Cayirci

www.liophant.org

Simulation Team

Objectives

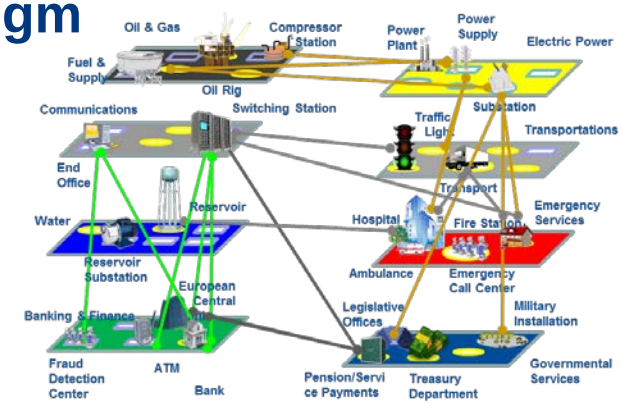


- *Identify the elements to model the Hybrid Warfare and the availability of existing models in this sector*
- *Development of Innovative Models open to address specific aspects such as Cyber Warfare*
- *Development of Innovative Interoperable Models to combine the concurrent action along the different layers*
- *Design of an Architectural approach for Interoperable Simulation in multiple domain able to evaluate alternatives in terms of flexibility, reliability and efficiency*
- *Development of a modular and scalable simulation for complex scenarios characterized by heavy computational workload.*

Simulation Team

Hybrid Warfare vs. Modeling

- the Hybrid warfare is a very significant field of application, considering that it addresses many different complex systems concurrently and requires to extend the understanding of the scenario over a wide spectrum of layers
- The modern term Hybrid Warfare is even controversial and its concepts could be consider present also in many historical cases, therefore nowadays, current modern technologies stress further the impact of this paradigm
- M&S in hybrid warfare scenarios represent the key methodology to investigate this field and to evaluate the impact of human factors as well as new layers such as cyberspace



Models Developed for Understanding Hybrid Warfare

In a hybrid warfare, the adversary uses all available means, even black side, to exploit the vulnerabilities of the defendant and to destabilize it.

Creating ambiguity, the denial and disabling the defendant in decision making are aimed in every action. The adversary tries to meet its objectives without an armed conflict even without a major change in its diplomatic and economic relations.

Two Pillars in Hybrid Warfare

The Adversary manages two parameters related to the defendant, namely the threshold and the willingness. It tries to keep the willingness of the defendant to clarify the adversary's intention and to engage in an armed conflict at the minimum possible level.

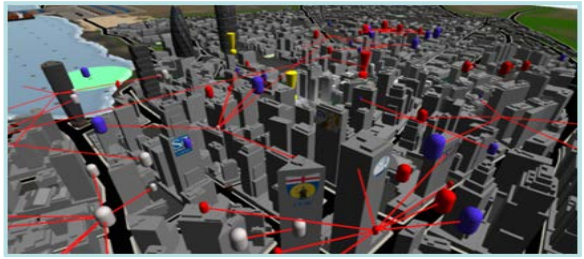
The willingness is strongly related to the international community's desire to support the defendant. When the willingness is over the threshold, the hybrid warfare is over one way or the other, i.e., either the adversary backs off or has to face an armed conflict with the defendant supported by the international community.

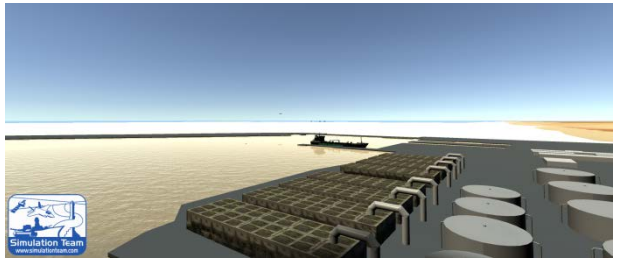
Therefore, the adversary does it's best to raise the threshold as much as possible without losing the control on the willingness.

Simulation Team

M&S Purposes in Hybrid Warfare

- ***Support to key decision makers in understanding the dynamics of Hybrid Warfare***
- ***Support identification of shortfalls and weak points in current organization, technological solutions, equipment and doctrine***
- ***Support to develop an effective approach to react to Hybrid Warfare in complex scenarios.***
- ***Evaluation of efficiency in critical situation enhancing the capability to understand the situation and risks related to different COA as well as trends in scenario evolution***

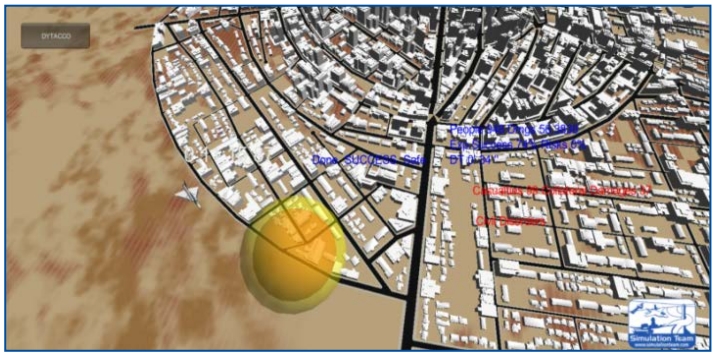




Simulation Team

Hybrid Warfare & Human Behavior Modeling

- In Hybrid Warfare it is crucial to reproduce the human aspects and relationships respect events and boundary conditions
- It is fundamental to model multiple aspects and layers including supply chain, transportation and energy that could be fundamental elements in hybrid warfare
- Human modelling results among the most important and interesting aspects to be addressed especially because all other layers influence this one as well as the final success or failure of the operations



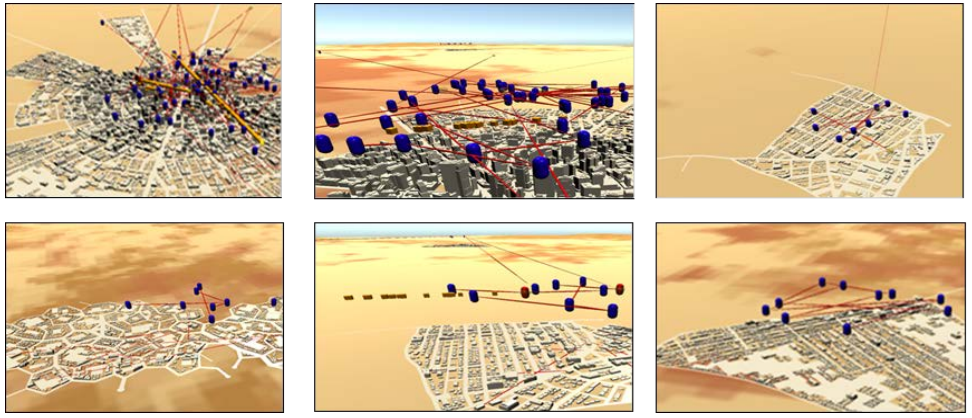
Simulation Team

Cyberspace and STRATCOM as Layers for Hybrid Warfare

Hybrid Warfare is often "confused" with Cyber Defense and it is not just a case

In facts the new layers such as STRATCOM and Cyberspace provide new opportunities to apply Hybrid Warfare concepts.

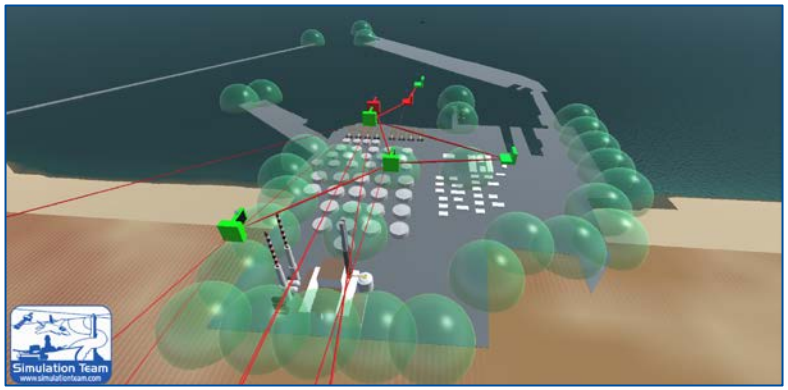
It is evident the necessity to develop simulators to cover this aspects and the potential to use Intelligent Agents in this context

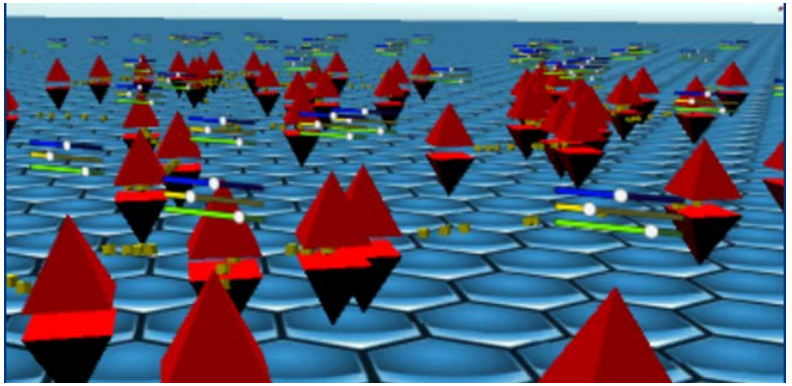


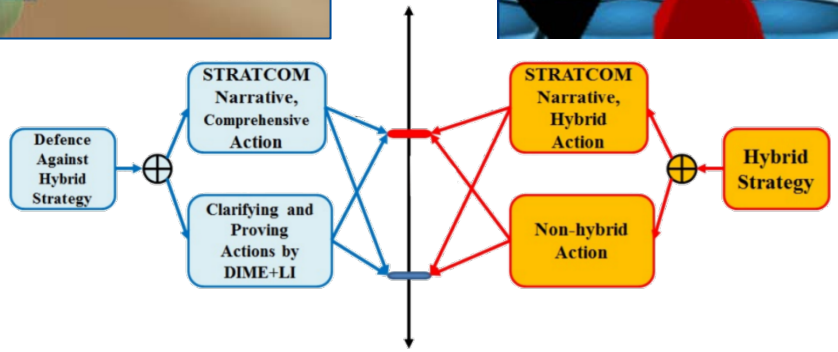
Simulation Team

NMSG ET-043
M&S for Hybrid Warfare

This Exploratory Team is devoted to investigate the potential of applied M&S. Currently we are developing different Simulation for Testing Concepts such as T-REX and CMHE







CMHE Model

Conceptual Model for Hybrid Environments

Different Models could be developed to address Hybrid Warfare Simulation. For Instance CMHE focuses on the definition of a conceptual model to describe Hybrid Conflict Environments.

Without the need of citing specific cases or countries, it is clear that hybrid strategy and warfare are becoming more important.

Hybrid strategies affect policy makers, military operations, economics and financial trends, intelligence and legal activities as well as information and media.

The CMHE is introduced to define and to gain further insight into hybrid environments. The model was implemented and tested by Monte Carlo Simulation to run experiments to provide evidence on its relevance.

Simulation Team

A Conceptual Model for Hybrid Warfare

CMHE Conceptual Model for Hybrid Environments

CMHE has been developed to investigate relationships between willingness & threshold

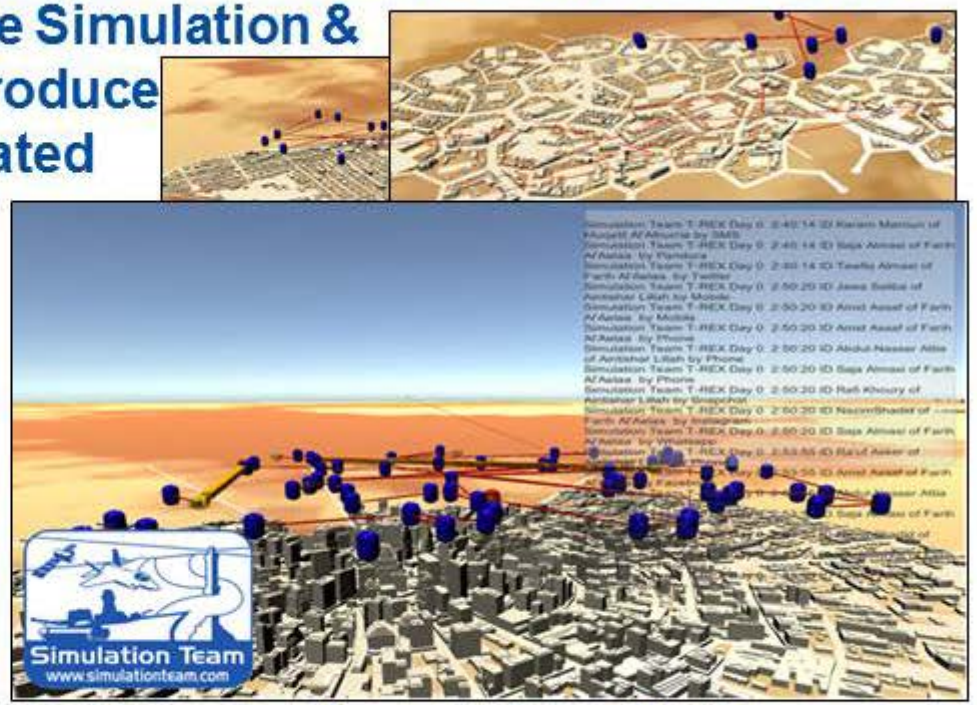
$$Capacity(\chi) = threshold(\tau) - willingness(\omega)$$

Simulation Team

T-REX

Threat network simulation for REactive eXperience

T-Rex (*Threat network simulation for REactive eXperience*) is a MS2G (Modeling, interoperable Simulation & Serious Game) devoted to reproduce Hybrid Warfare and to be federated with other elements to evaluate the impact of these actions.



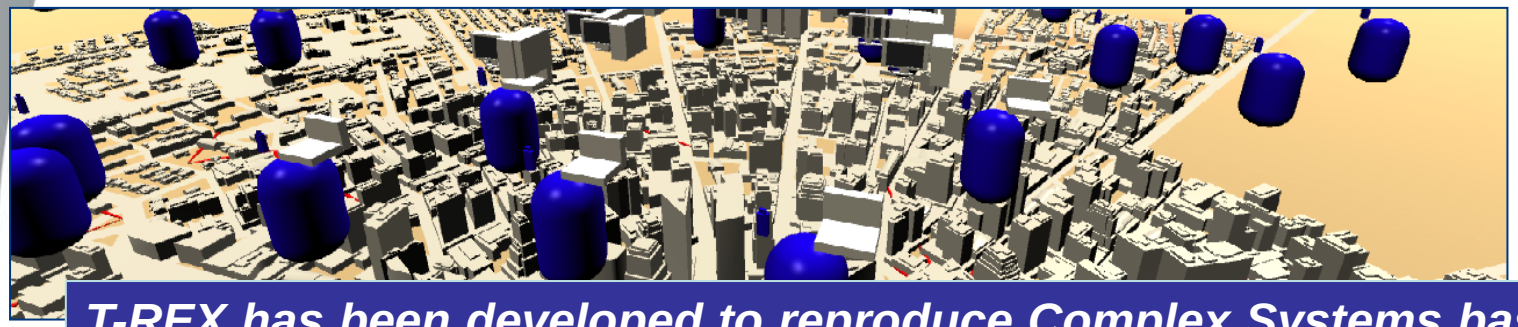
T-REX reproduces urban, as well as extra urban contexts over multiple domains including land, air, sea, space and cyberspace. The models allows to consider media communications and possibility to use different assets and to experiment virtually the different decisions in terms of COAs (Courses of Actions)

Simulation Team

T-REX: A MS2G Simulation for Hybrid Warfare



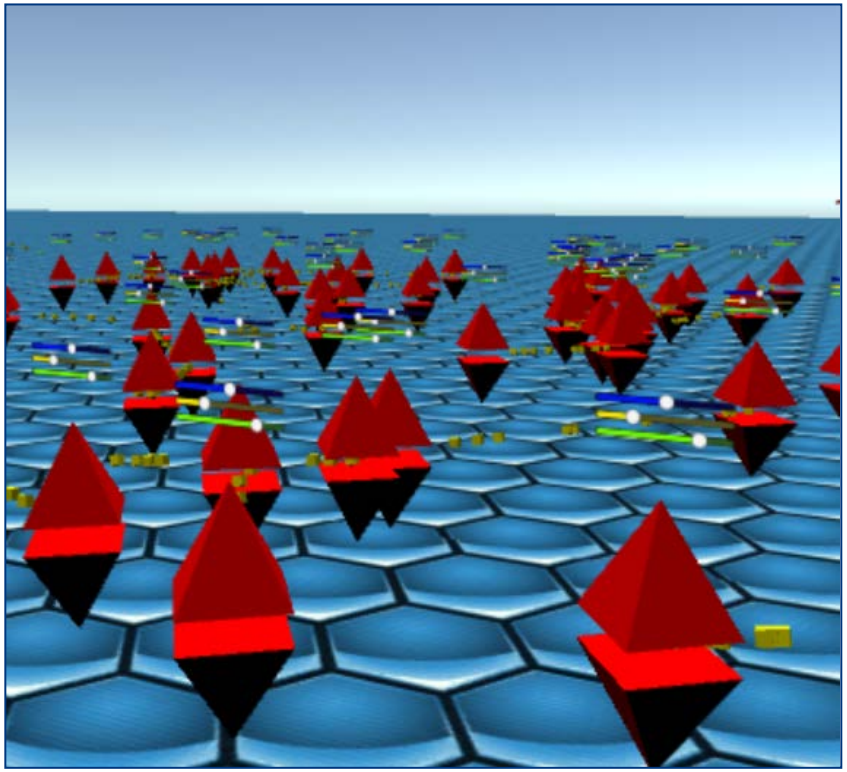


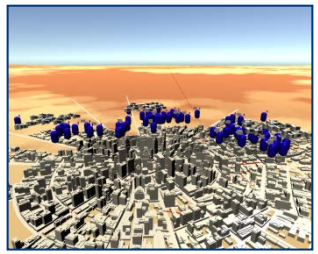
T-REX has been developed to reproduce Complex Systems based on Agent Driven Simulation including Cyberspace, Population, Threat Networks


T-REX Developments

- Simulation Team developed IA-CGF (Intelligent Agents Computer Generated Forces) to address multiple sectors and a new NCF (Non-Conventional Framework) addressing Hybrid Warfare has been experimented
- T-REX was presented and demonstrated during NMSG ET-043 as an example of the potential of M&S in this sector.



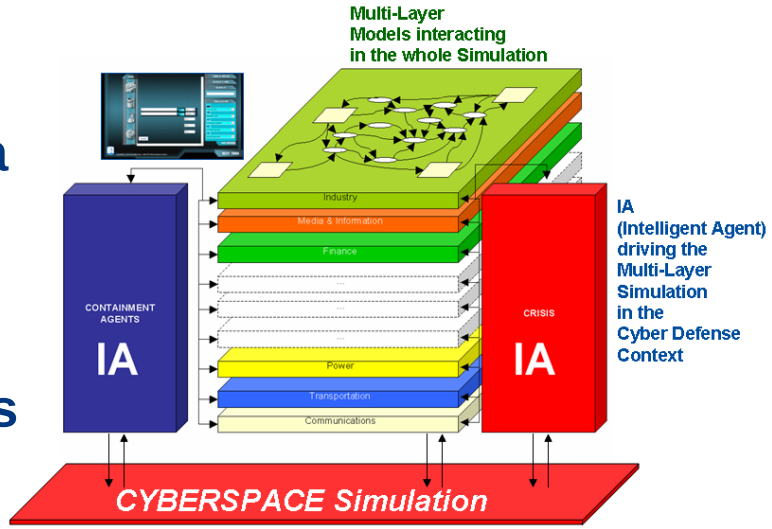
T-REX and MS2G Paradigm



- T-REX (Threat network simulation for REactive eXperience) adopts MS2G paradigm (Modeling, interoperable Simulation & Serious Game) that combines Complex System Modeling and intuitive Serious Game framework.
- T-REX is a stochastic discrete event virtual interoperable simulation able to perform fast time runs in order to evaluate vulnerability reduction as well as risk assessment respect hybrid warfare scenarios.
- T-REX includes metamodels dedicated to reproduce specific aspects (e.g. communications) that could used for fast simulation or substituted by federating details models made by specific tools (e.g. an OPNET simulator reproducing in details the communication protocols and hardware devices)

T-REX Multilayer Approach

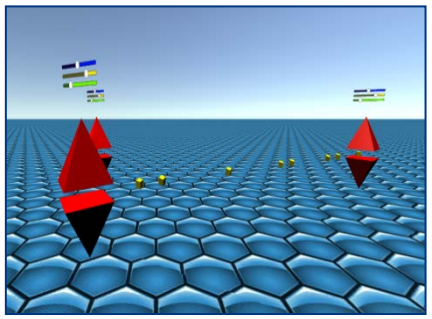
- The T-REX approach reproduces multilayers including social, economic, military.
- For instance the context on multiple layers including people objects (single individuals and/or families) and interest groups (e.g. one political party, a leader, an industrial association, a religious group, a social class), each one with its own social network and mutual relationships.
- T-REX includes also other layers such as technological one as power grip, communication networks, transportation network



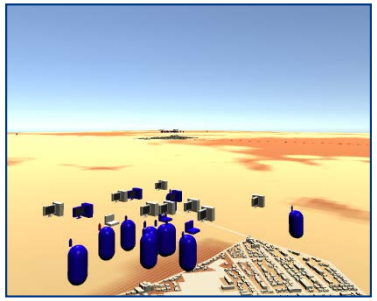
Multilayer Approach in Modelling Cyber Defense as Fifth Dimension interacting with Strategic Assets

T-REX and Cyberspace

- Cyberspace is modeled as a corresponding space to the ICT (Information and communications technology) with a topography related the logic and structure of the configurations and interconnections.
- Cyberspace in T-REX is constituted by nodes and links, characterized among the others, by the Integrity, Availability and Confidentiality Levels that evolve dynamically for each element
- by this approach it becomes possible to conduct actions on cyber elements (e.g. an IP Address, a PC) and see the effects on the operational layer as well as on the social one.



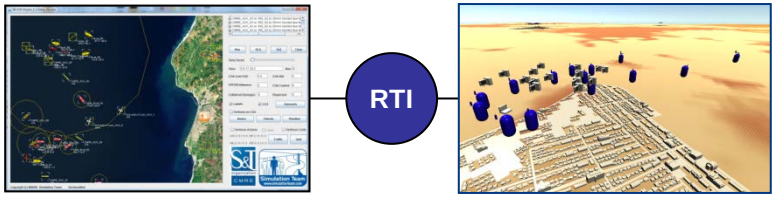
T-REX and IA-CGF



- T-REX is used to simulate urban, as well as extra urban contexts over multiple domains including land, air, sea, space and cyberspace
- T-REX elements are driven by the IA-CGF that act and react based on their perception about the situation awareness and the boundary conditions
- The IA-CGF and different T-REX metamodels guarantee the possibility to consider media communications and to evaluate different assets by experimenting virtually alternative decisions in terms of COAs (Courses of Actions) within an Hybrid Warfare Scenario.

Simulation Team

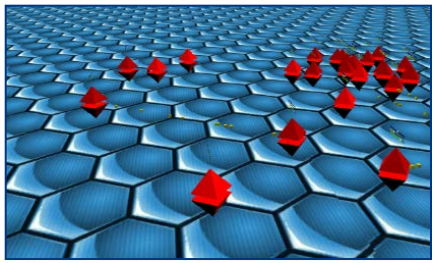
T-REX & HLA



- The native HLA (High Level Architecture) structure of T-REX simulator guarantees Interoperability and allows to keep this environment open for being federated with other simulators
- T-REX has been already tested integrated with JESSI (Joint Environment for Serious Games, Simulation and Interoperability), a virtual interoperable environment with many different models to simulate complex heterogeneous networks including traditional and autonomous platforms (e.g. UAV, USV, UGV, UUV, Vessels, Aircrafts, land vehicles, missiles, etc.) that operates over a joint scenario (i.e. air, land, sea, space, cyberspace) and with SPIDER (Simulation Practical Immersive Dynamics Environment for Reengineering)

Simulation Team

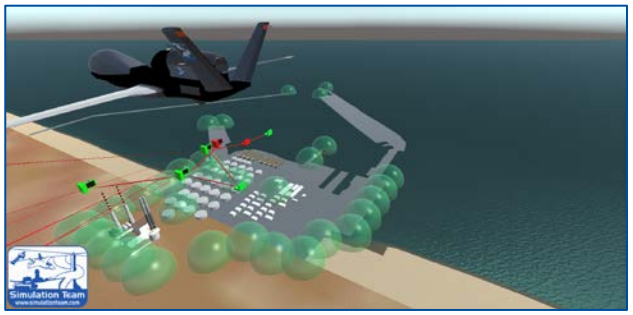
T-REX Demo



- The demonstration of T-REX at ET-043 (Hybrid Warfare M&S) is based on a scenario reproducing threat networks, suspects and population over a small region and their behavior driven by IA-CGF based on their status, human behavior modifiers (HBM) and their specific life cycle.
- The scenario included a medium size city, four small towns within a desert area facing the sea; on the coast near the major town it was simulated a small port with an oil terminal, a tank farm, a desalination facility with multiple units, a power plant and the related security system (e.g. perimeter sensors/cameras/defenses, ICT Network).

Simulation Team

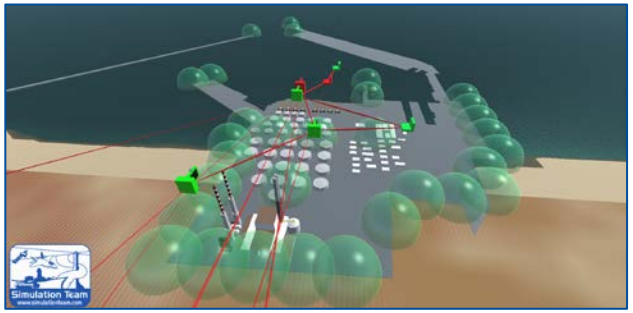
T-REX Demo Actors



- The demonstration of T-REX included Population, Threat Network, Media Communication, Traditional Assets as well as Different Autonomous Systems, Critical Infrastructures
- For instance UAV (Unmanned Autonomous Vehicles) in ISR (Intelligence, Surveillance, and Reconnaissance) are respect threat network.
- The cyber layer of T-REX in this case included computers, laptops and mobile IoTs (internet of Things) as well as firewalls and procedures.
- The threat network was composed by terrorist agents able to adopt different operative modes such as “sleeping”, “stand by”, “planning action”, “preparing action”, “executing action” on different layers.

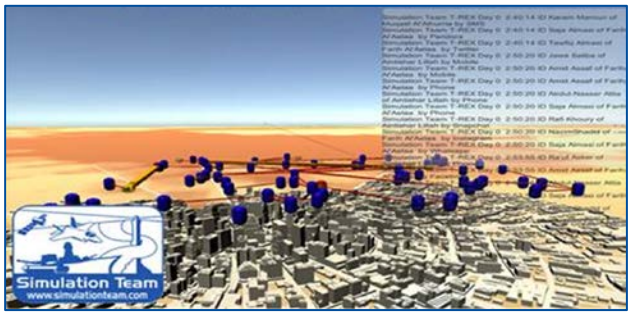
Simulation Team

T-REX Threat Example



- In the simulation, an example of attack is based on diffusion of an a sleeper virus, installed over a flash memory, infecting and affecting integrity just on specific systems. The goal of the virus is to compromise just on specific servers (i.e. Port Security Server) accessing it from an infected computer through a remote supervisor access.
- The demonstration allows to reproduce the diffusion of the virus and the actions of the threat networks as well as the opportunities to capture the spill of information by the JISR as well the evaluation of the impact of the attack to study vulnerability reduction, impact on population and effectiveness of offensive and defensive actions over the different layers.

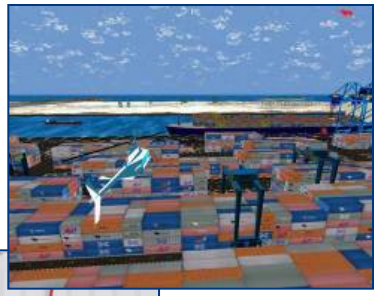
Conclusions



- **T-REX simulator represent an example of the potential of using advanced intelligent agents and multi layer modeling in reproducing Hybrid Warfare scenarios even to evaluate and test hypothesis and assumptions related to vague or uncertain factors.**
- **the demonstration confirmed the importance to be able to conduct vast experimentation and define the criteria to create the scenario based on the available information and on the different hypotheses**
- **by this approach it becomes possible to evaluate symptoms and to study impacts of actions and reactions as well as to analyze their consequences respect interest groups, population and social-economic-political tissue.**

Simulation Team

References



DIME Genoa University
via Opera Pia 15
16145 Genova, Italy
www.itim.unige.it
Agostino Bruzzone
agostino@itim.unige.it

Simulation Team
Viale Molinero 1
17100 Savona, Italy
www.simulationteam.com
Riccardo di Matteo
dimatteo@simulationteam.com

.... Questions?