Simulation Team

Modeling & Design of Complex System

Cyber Threats

Liophant Simulation

M&S Net

MITIM Simulation Team Genoa Center

McLeod Institute of Technology and Interoperable M&S
Genoa Center

Agostino G. Bruzzone

agostino@itim.unige.it

www.simulationteam.com
www.liophant.org
www.itim.unige.it/strategos

DIPTEM
University of Genoa

Simulation Team

Who's Who
Agostino G.Bruzzone

- Basic Engineering Studies in Italian Naval Academy, Pisa and Genoa University
- Mechanical Engineer
- Expert in Modelling & Simulation, Project Management, Operation Management, AI & IA, Industrial Plants &Logistics
- Expertise as Freelance Consultant for Industries, Companies, Ports, etc.
- Experience in Projects with Major Companies (i.e. IBM, LMC, Boeing, FCA, Ansaldo, Leonardo, Solvay) & Agencies (i.e. EDA, NASA, NATO, DGA, DoD, Navy, etc.).
- Full Professor in DIME, University of Genoa
- Visiting Professor in Several Universities in North & Latin America, Europe, Australia, Africa and Asia
- World Director of the M&S Net (34 Centers worldwide) & Director of McLeod Institute of Simulation Science Genoa
- Founder & former Leader of the Simulation Program of the NATO STO CMRE
- Project and Program Manager in R&D Initiatives & Joint Ventures with Industries & Agencies for several MUSD along last years
- Director of the Master Program in Industrial Plants & MSc STRATEGOS in Strategic Engineering of Genoa University
- President of Liophant and Simulation Team
- General Chair of major conferences (e.g.I3M)

Simulation Team

Cyber Threat Examples

Lets look at some Examples…

Lets look at some Examples…

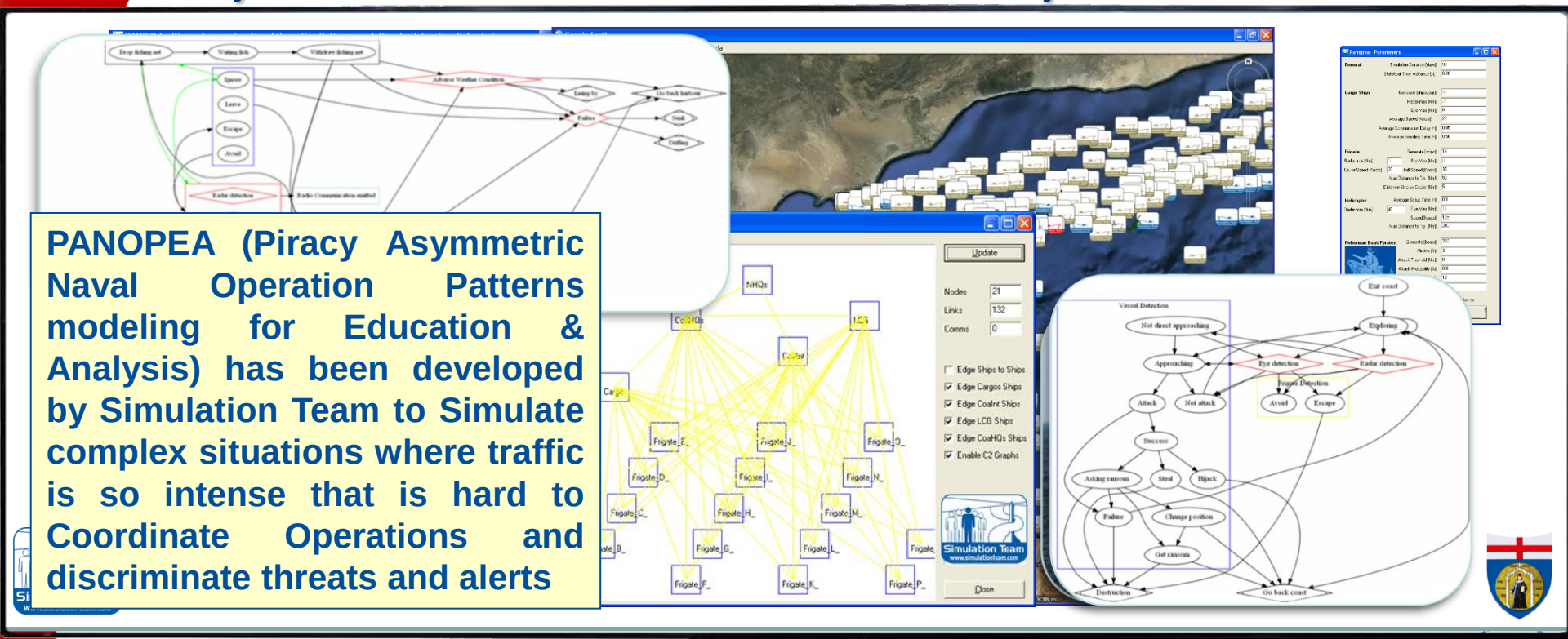
Lets look at some Examples…

Working on Real Virtual Worlds

Digital Twins are currently an opportunity, but even an issue considering potential new threats and this is real since many years on cyber layer.
This point turns to be critical as soon as the Cyber and Real world interact on critical assets

IA-CGF for Large Systems & Huge Interactions

Piracy models included since first decade of 3rd Millennium Cyber Defense Issues



PANOPEA (Piracy Asymmetric Naval Operation Patterns modeling for Education & Analysis) has been developed by Simulation Team to Simulate complex situations where traffic is so intense that is hard to Coordinate Operations and discriminate threats and alerts

Simulation Team

Haiti Humanitarian Support Demonstration

We Rebuild the Bridge! Go Great Genoa!
LIBERTAS
Che l'inse?

Consider the huge impact and low effort of Cyber Defense on Humanitarian Crisis… and face it

The demonstration was devoted to show the potential of interoperability in combining different simulators for full coverage of a complex problem such as that one of Haiti. Simulation Team was involved by using his interoperable IACGF reproducing Population Behavior, Human Factors (famine, stress, diseases, fear, aggressiveness), Riots and Gang Activities as well as the impact of the Simulation Earthquake

- JTLS
- JCATS
- IA-CGF Riots
- IA-CGF EQ
- VBS2
- DI-GUI
- PLEXSIS

Simulation Team

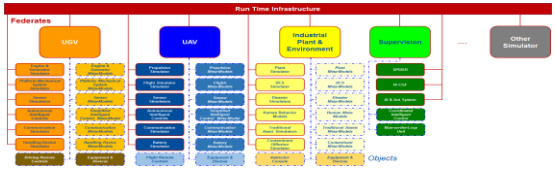
UxV & Plants…
…and more!

We Rebuild the Bridge! Go Great Genoa!
LIBERTAS
Che l'inse?

New Autonomous Assets, also in Industrial Environments, enhance the impact of Cyber World

Inspection Outside

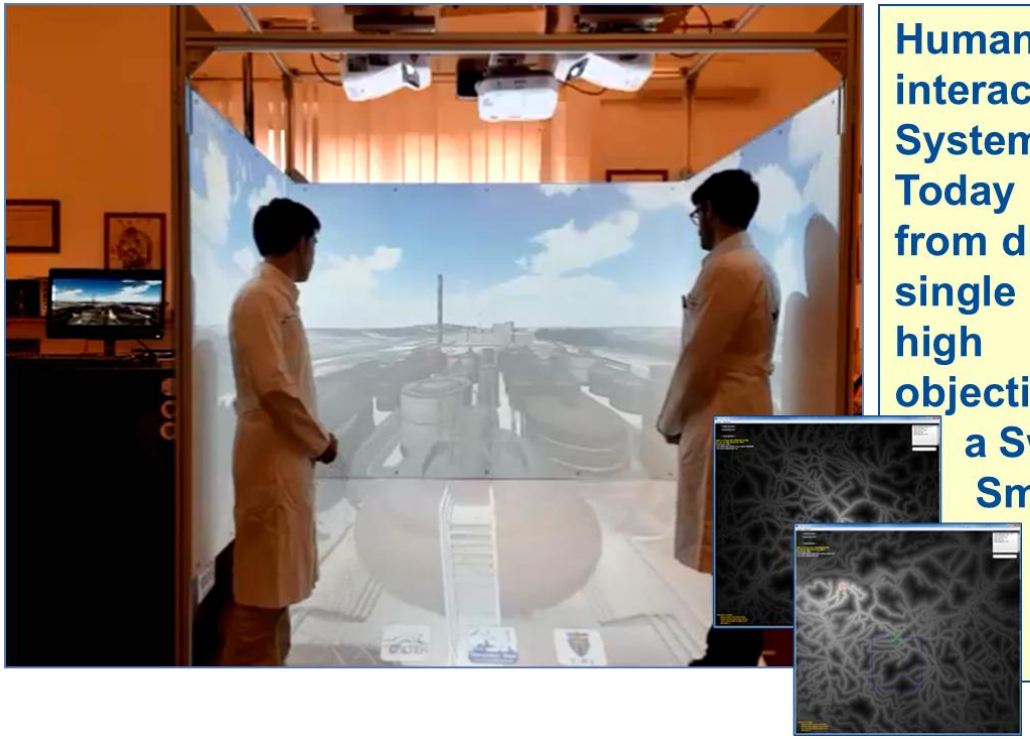
Inspection Inside



UxV Unmanned any domain Vehicle

AI & Man on the Loop vs. Man in the Loop

AI are fundamental in study and addressing the Cyber World and new Assets of Physical World



Humans need new ways to interact with Intelligent Systems.

Today we need to pass from driving and piloting a single UAV to assigning high level task and objectives to a Wing or a Swarm of Uxv.

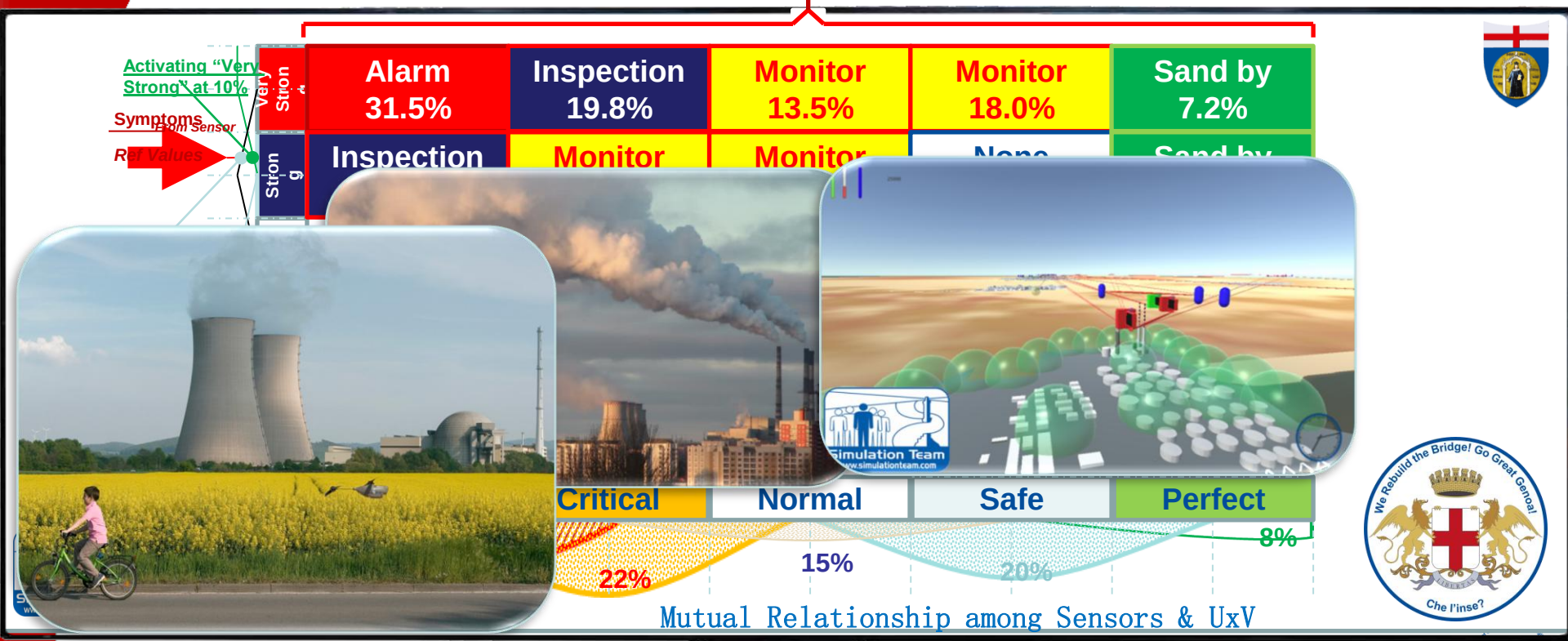
Smart Simulation allows to Design, Experiment & Test these new Solution

Simulation Team

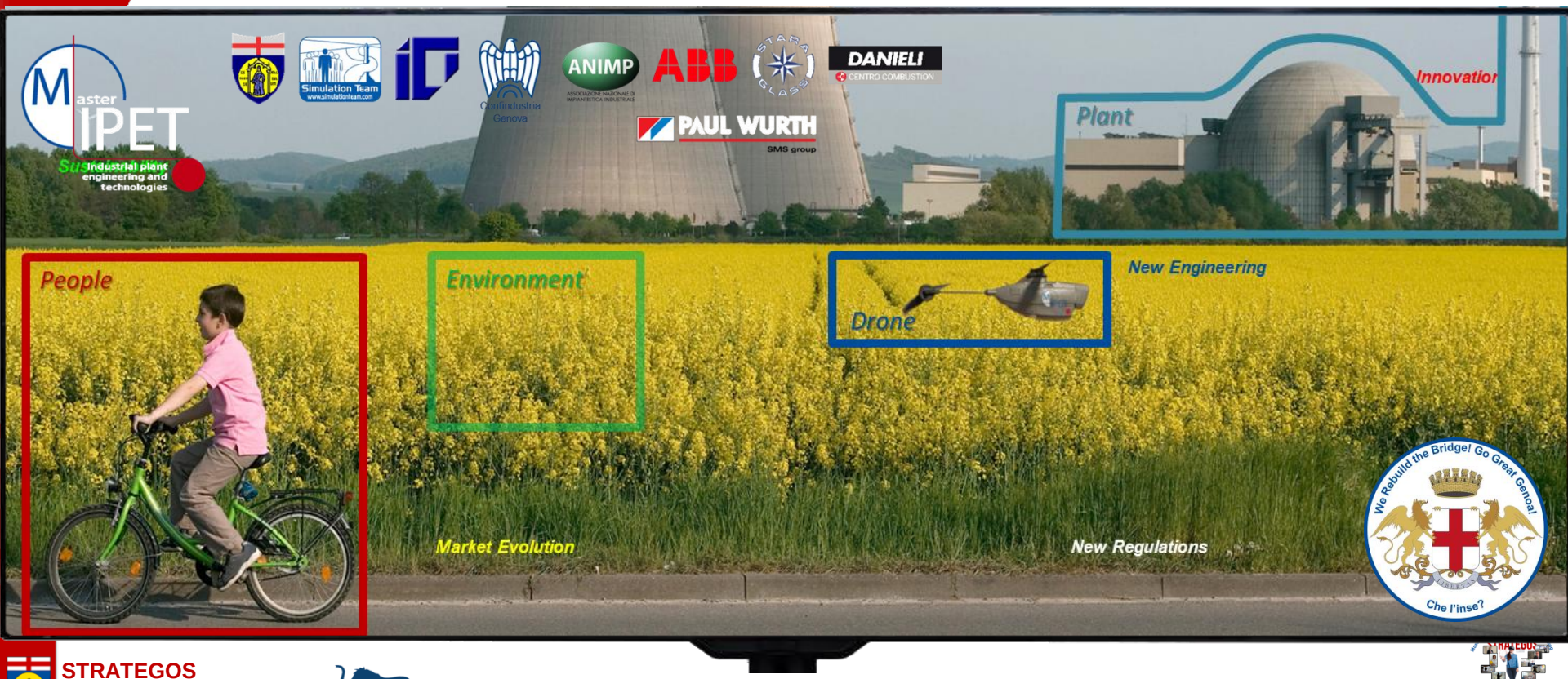
AI… Artificial Intelligent for Awareness driven Initiatives

Danger	31.5%
Inspect	35.2%
Monitor	23.3%
Stand by	8.0%

General Situation on the Plant



MS2G supporting us during good times..



…and during Crisis and Critical Conditions

We need Smart Simulation in Engineering

…because things are Changing!

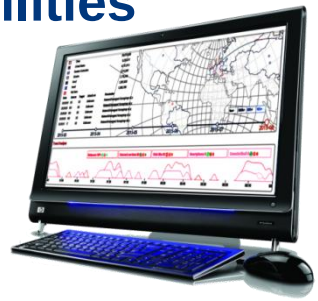
Simulation Team

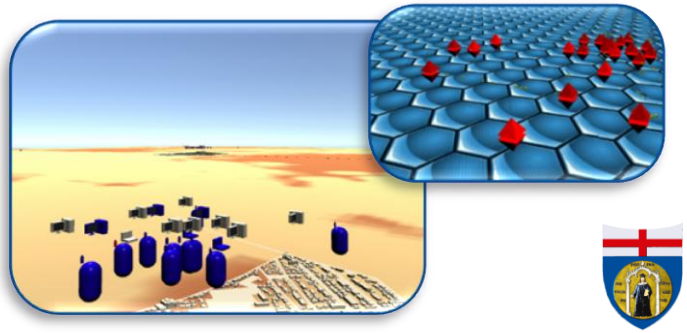
Cyber Domain: adding Spices to T-REX

Threat network simulation for REactive eXperience

T-REX, one of most advanced Cyber Warfare Simulator, has been developed by Simulation Team

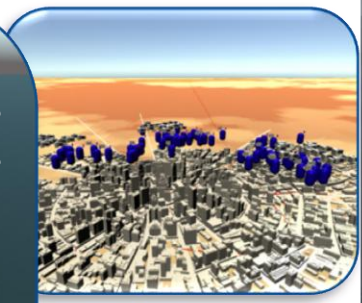
The Cyber Security is part of T-Rex environment and allows to evaluate the impacts on operations and estimates their magnitude This approach allows to considerate the Cyber Domain Complexity and the impacts on ICT process and infrastructures as well as Social Engineering elements. The MS2G (Modeling, interoperable Simulation & Serious Games) approach, make possible to raise users awareness and improve performance reducing vulnerabilities

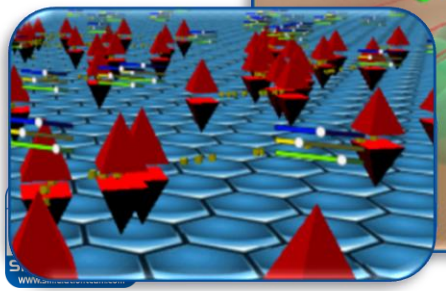




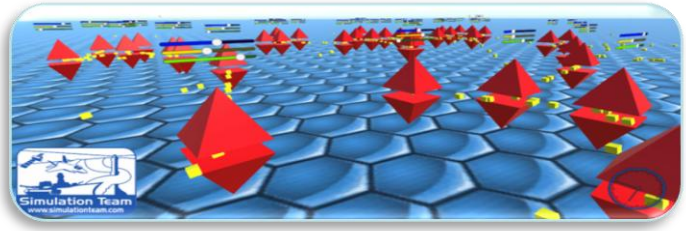
Hybrid Challenges & Autonomous Systems

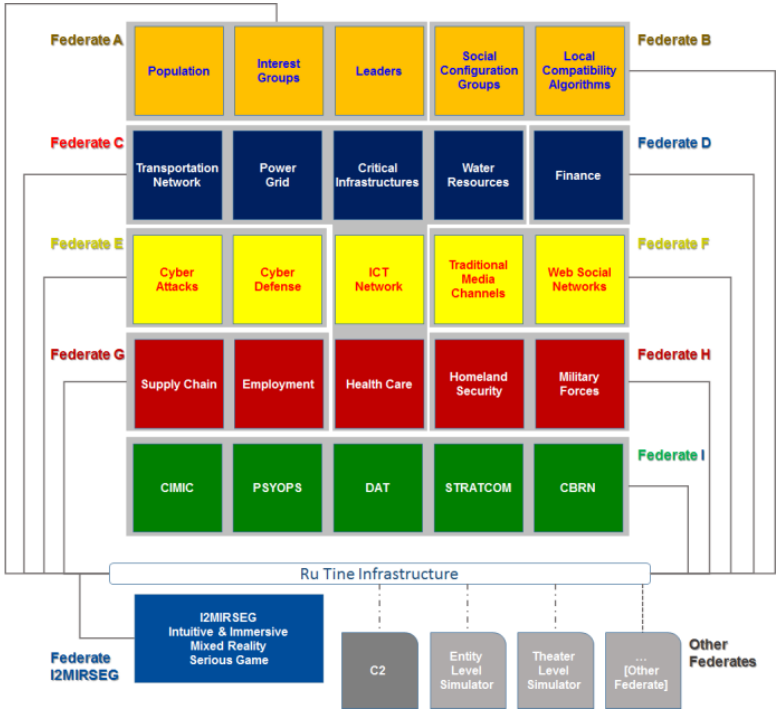
Autonomous Systems represent crucial elements for Hybrid Challenges both in terms of available Resources and Threats The T-REX simulates towns, infrastructures, people, UxV as well as Cyber & Real coordinated actions that affect whole System





Creating Comprehensive Environments





Simulation Team

New Frontiers &…

We Rebuild the Bridge! Go Great Genoa!
LIBERTAS
Che l'inse?

There are Sharks in these waters?

Yes, there are Sharks in all Seas!

Cyber is …
Everywhere

88 Shark Attacks *World/year*
5 deaths in 2017

230'000 Malware produced by day
77'183 Cyber Severe Damages
Cyber Insurance Premiums 1.3bUSD
Cyber Security Gov.Budget 28bUSD
…just USA …already 3 years ago

Simulation Team

New Frontiers &…
…New Engineers

We Rebuild the Bridge! Go Great Genoa!
LIBERTAS
Che l'inse?

Problems are know but Often Decision Makers are not ready!

April 29, MMXIX, 0607 Z

Cyber Attacks are able to disable official websites and networks, disrupt or disable essential services, steal or alter classified data and cripple strategic assets & critical infrastructures such as Communications, Power, Transportations, Finance, Health Care.

Cyber Attacks are addressing both Civil and Military Targets

Cyberwarfare is a Cyber-based Conflict involving motivated attacks on information and information systems.

Real Crises were there in Real World

Big Data are a resources also for Attackers in Cyberspace

- Yahoo 2013 & 2014, Over 1 billion accounts
- TJX, 2003, 45.7 million credit/debit cards, driver's licenses
- FriendFinder, 2016, 412 million accounts on dating
- Ebay, 2014, 145 million accounts
- Heartland Pay.Syst, 2008/2009, 130 million credit cards
- Target Stores, 2013, 110 million records compromised
- Sony OE., 2011, 102 million records compromised
- Anthem, 2015, 69 million health insurer records
- Home Depot, 2014, 56 million credit and debit cards 10.5 GUSD (~194 USD/card)
- LinkedIn, 2012, 6.5 million accounts (4%), password cracking in 72h for 90% cases

Simulation Team

Attacking not C2… but your Plug

We Rebuild the Bridge! Go Great Genoa! LIBERTAS Che l'inse?




MiTM Man in The Middle Dsniff Dug Song Sniff through SSH & HTML by MiTM

It is not necessary to attack your PC or Mobile…

… new Kitchen Appliance provide new vulnerabilities:

- To get your Google Account by MiMT from a Fridge able to propose you the Google Calendar (2015)
- To generate a Junk Mail Campaign spamming 750'000 emails from 10'000 Home Devices (2014)
- To watch your home from Always On Camera from Smart TV (2015)

Smarty Federal Trade Commission

Kids want to have Fun and test Toys

- Estonia, April 26-May 23, 2007, DDS, Botnet, Ping floods: All Government, 2 Banks, Political Parties, No Parliament Email, No Credit Cards, no ATM
- Georgia, August 7-12, 2008, DDS, Botnet, Web Defacement, Sql Injections, Spamming: News and Government Websites Down, Gov.Comms down with the World, Banks & Cell Phones down.
- Kyrygistan, January 18-31, 2009, DDS, ¾ IPS down, 80% internet down, mobile down
- Ukraine, 2015/2017, SCADA,Blackouts 1 million People 2h

Simulation Team

Do you stuck your Password on the Fridge?

It is not necessary to attack your PC or Mobile… new Kitchen Appliance provide new vulnerabilities:

- To get your Google Account by MiTM from a Fridge able to propose you the Google Calendar (2015)
- To generate a Junk Mail Campaign spamming 750’000 emails from 10’000 Home Devices (2014)
- To watch your home from Always On Camera from Smart TV (2015)

MiTM Man in The Middle Dsniff Dug Song Sniff through SSH & HTML by MiTM

Simulation Team

HVAC: you will feel Hot not at the Office… but in your Wallet

A major cyber attack on Target, a major USA Retailer, started by **Malware-laced Phishing Emails** sent to **employees of a supplier** of HVAC systems. This vendor had access to Target's network login credentials to **remotely monitor temperatures & energy consumption** in stores where the HVAC systems were installed. The phishing attack **turned up those credentials**, so the hackers used them to **access the store's corporate network** and, specifically, the **company's payment systems**. This is an example of a devastating low-tech simple attack.

Power Building… Vulnerable

- **Primary Power Systems**
  - Switchgear, Power Panels, PLC's
- **Backup Power Systems**
  - UPS, Power Distribution Units, Generators
- **Mechanical Systems**
  - Chillers, Air Handlers, Cooling Towers, Boilers
- **Building Management Systems**
  - BMS, EMS (Energy Mngt System, DCIM (Data Center Infrastructure Management)
- **SCADA** (Supervisory Control And Data Acquisition) **Systems**

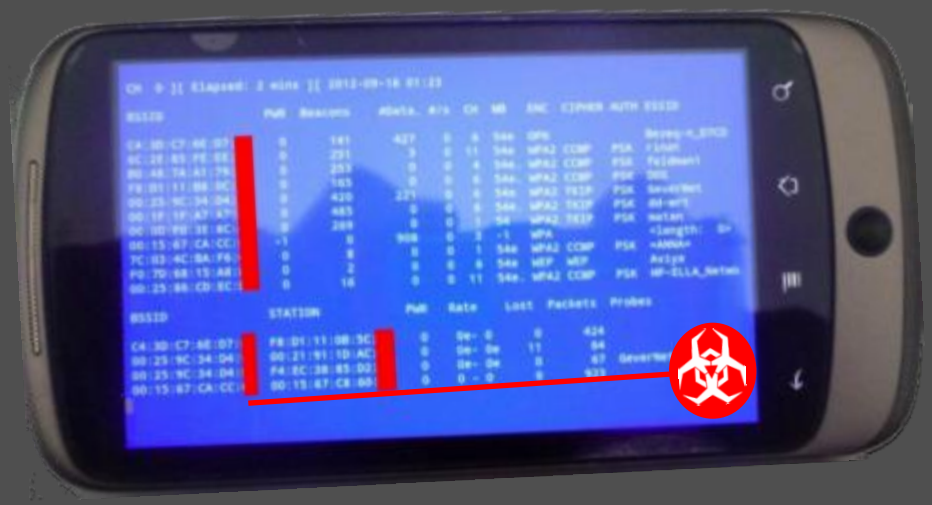
Example
Power Control Systems

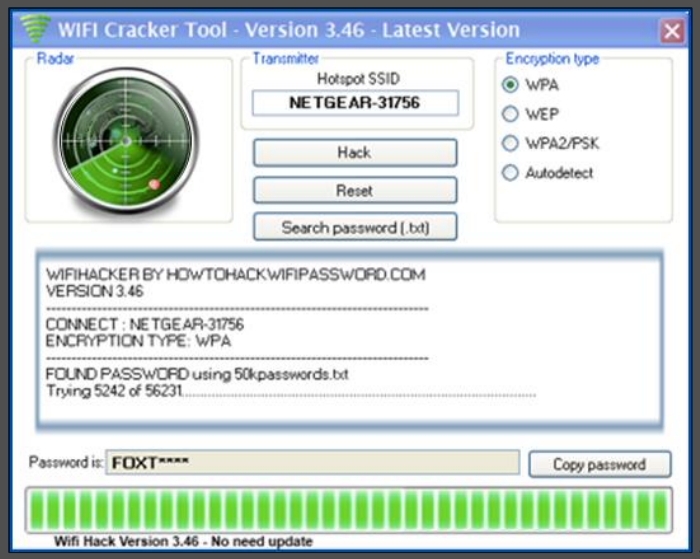
- SNMP (Simple Network Management Protocol) are often vulnerable to Spoofing
- PLCs (Programmable Logic Controller) allow hackers with modest skills to access them and take control of switchgear in absence of firewalls

… & WiFi: Lighting Vulnerable

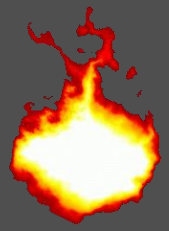
- WiFi technology is extensively used in Domotics for instance WiFi lighting systems use WPA2 encryption feature

- New generations of WiFi Crackers is usually successful in 99% in breaking these systems and give access to the control



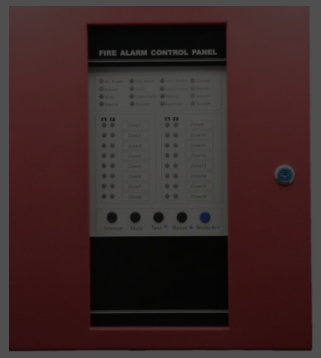


Blackout & Darkness… not only… even Fire!



- Ethernet network is a fairly new form of communication for fire systems. National Fire Alarm and Signaling Code (NFPA 72) covers the requirements for networking fire panels and control systems and it requires that all segments be separated and secured. NIST (National Institute of Standards Testing) identified Risks on new Fire Control Panels suggesting to add security barriers on HW layer.

- Indeed, some Fire Control Panel provide services by emails Simple passwords over HTTP are at risk of interception and email accounts could be easily captured. Once compromised it is possible to access configuration files, circumventing all fire panel system security.



- WannaCry, EternalBlue, Petya, etc. could affect these systems if not protected.

Traffic Jam… is it Real… …or Cyber?

- Two Students from Technion, the Israel Institute of Technology, proposed a Real Traffic Jam attacking phony Waze GPS Apps (Google owned) by creating a massive Fake Traffic jam by Fake Users forcing the system to reroute people within same area (2014)

- Carmel Tunnels were blocked creating an Huge Block in Haifa Car Traffic by hacking Camera Systems that put the tunnel in lockdown mode (2013).

The Attacks were based on two phases:

- Traffic Block of 20' on "day 1"
- Traffic Block of 8 h on "day 2"

Just Data & Money? Safety?

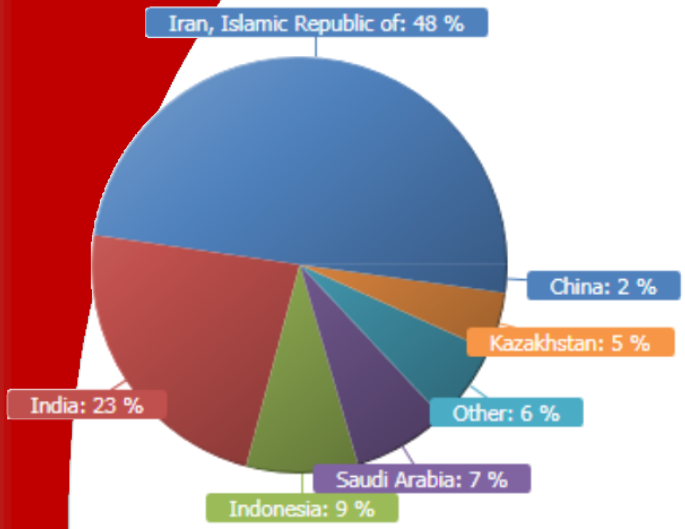
University of Texas compromised GPS of a 80MUSD Yacht by spoofing using a 2k$ device…

Italian Coast
August 2013

- **18/11/2017** Aeigs DD USS Benfold vs. Tugboat
  Sagami Bay: Minor Damages, Side Scratches
- **21/8/2017** Aeigs DD USS John S. McCain vs. MC Ship 50000DWT
  East of Singapore: 10 Casualties, 3 Injuried, Severe Damage
- **17/6/2017** Aegis DD USS Fitzgerald / MC Container Ship 40000DWT
  East of Singapore, 7 Casualties, 3 Injuried People, 10 MUSD Damages
- **9/5/2017** Aegis CG USS Champlain / South Korea Fish Boat (20m)
  Sea of Japan, No Injuries, light Damages
- **31/1/2017** Aegis CG USS Antietam, Anchor Dagging, Prop.Out Control
  Tokio Bay, No Injuries, 4 m^3 oil spill, Propellers Damages

STUXNET
36 Months Later

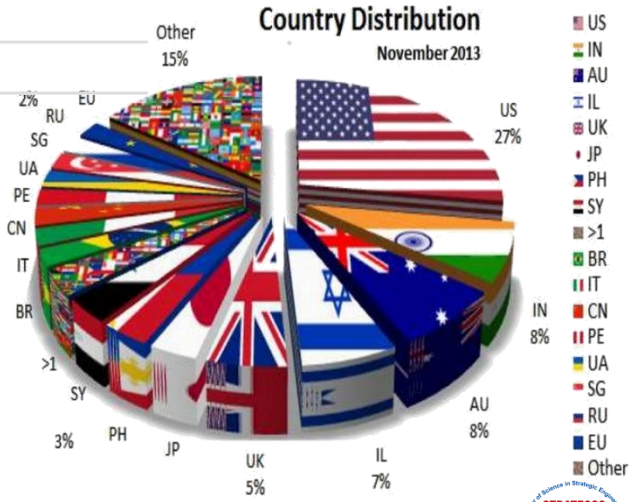
Geographical distribution of Stuxnet infections 2013-2014.



Percentage	Infection Records	Trojan
47.71	198	Iran, Islamic Republic of
23.13	96	India
8.67	36	Indonesia
7.47	31	Saudi Arabia
6.27	26	Other
4.58	19	Kazakhstan
2.17	9	China

Country distribution of Stuxnet infections 2013-2014.

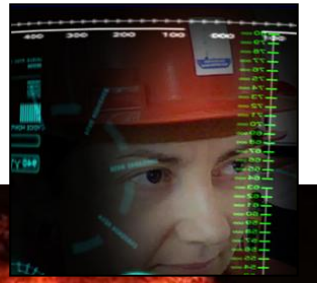
- **Discriminating Targets and adopting Deception and Sabotage on Hardware**



- **SCADA (Supervisory Control and Data Acquisition.) are so infected that 36 months after the attack there still major contaminations**

Cyber & Safety in a Steel Mill!

- Industrial Plants are plenty of Automation and extremely exposed to Cyber Attacks as much as turn to be distributed Systems (e.g. DCS, ICS, SCADA Systems)



- It is not only about stealing data or strategic attack to nuclear facilities

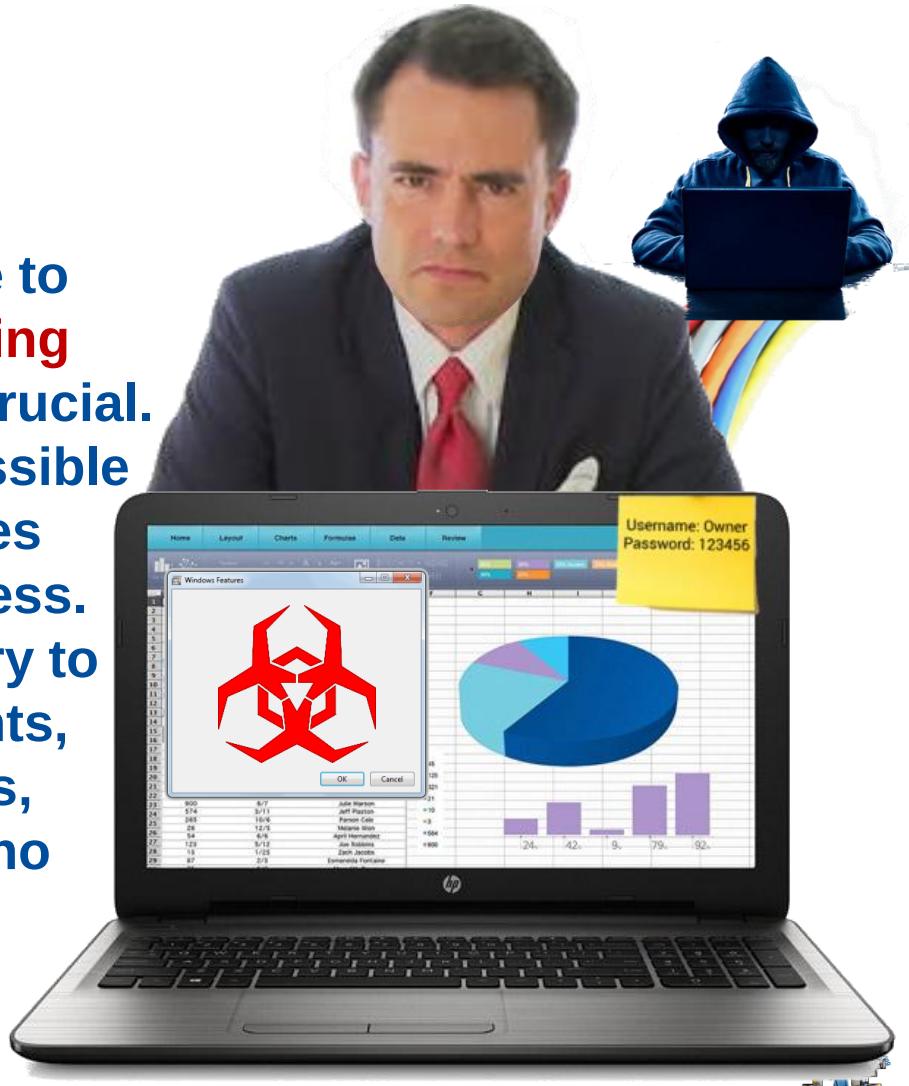
- A Steel Mill has been attacked in Germany with severe damages to the Plant, potentially with high risks for Human Safety

BSI, December 2014 APT Attack to Steel Mill

DCS	Digital Control Systems
ICS	Industrial Control Systems
SCADA	Supervisory Control And Data Acquisition

Risks from Outside…

and Inside!



BMS vulnerability is no only due to external attacks: Social Engineering and safeguarding from within are crucial. BMS are often multi-user web accessible This provide additional functionalities And use but introduce cyber weakness. To secure the systems it is necessary to reengineer process, manage accounts, control privileges. Expiring accounts, disabling immediately employees who leave as well as changing accounts when people switch roles are good practices to address some issues.

Ignorance & Lack of Awareness are major Weakness

Due to the evolving, diverse & complex nature of BMS and EMS, many system owners simply do not know where to start when it become necessary to define a cyber security strategy. Lack of Awareness about their vulnerability state means that the effective application of security technology or process is not possible. Many customers have difficulties in determining vulnerability levels, exposure, and possible impacts as well as the inability to monitor who has access to networks and critical assets. They face difficulties also in distributing and enforcing appropriate policies and procedures.

Thinking bad…

HVAC overheating Server Room

Fake Alerts on Speaker & Panels create Panic

Fire Control & BMS blinded during Fire

Intrusion via BMS In Company Tlc System

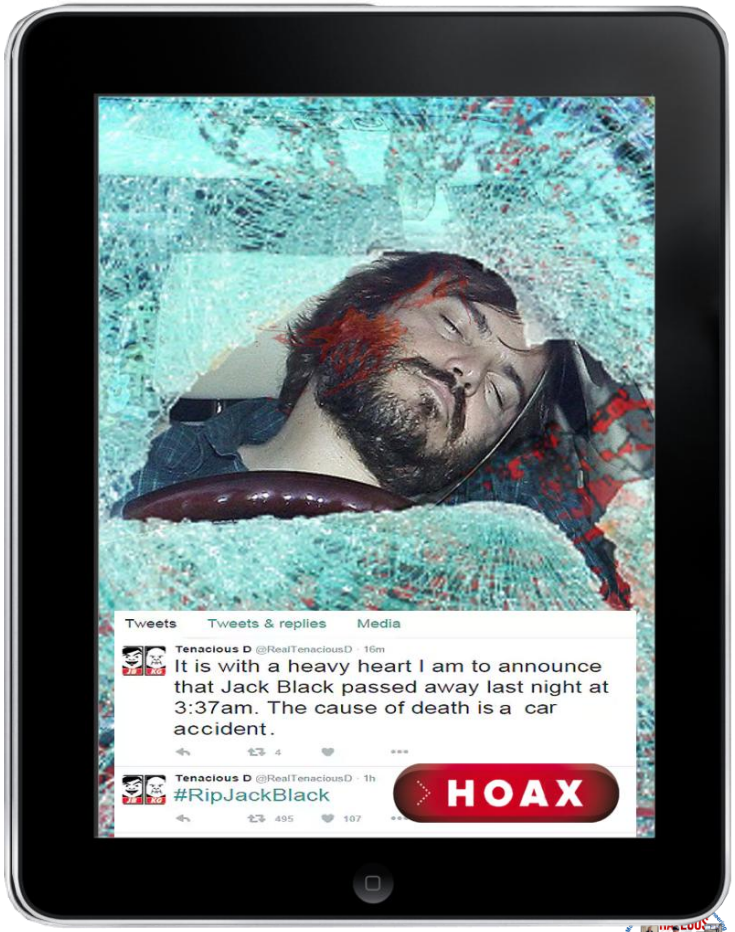
You don't need to Blow a Bomb… just a Fake New

- Society and People are very vulnerable to Deception & Fake News.
- Social Media reinforces these risks and requires Models to be able to evaluate the consequence of these events

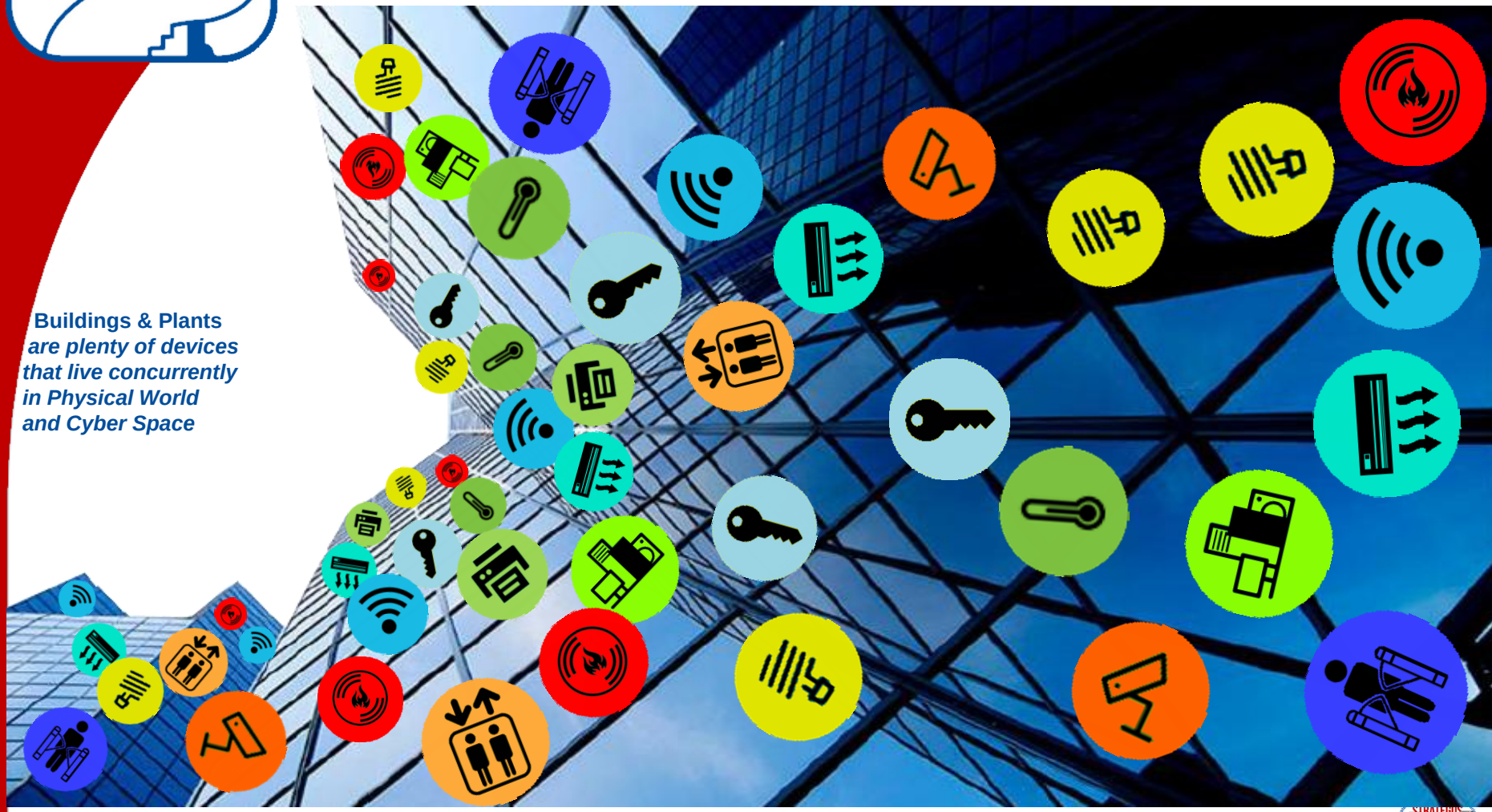
1500 Injured People in few second for Panic during a Social Event

Social Networks… Vulnerabilities & Simulation

- Injection of Fake news is very easy and could change attitude of people
- It is important to simulate Population dynamic reactions to Scenario Evolution on Social Networks, driven by Intelligent Agents
- It is necessary to simulate the impact of fake news and other media attack and population reactions



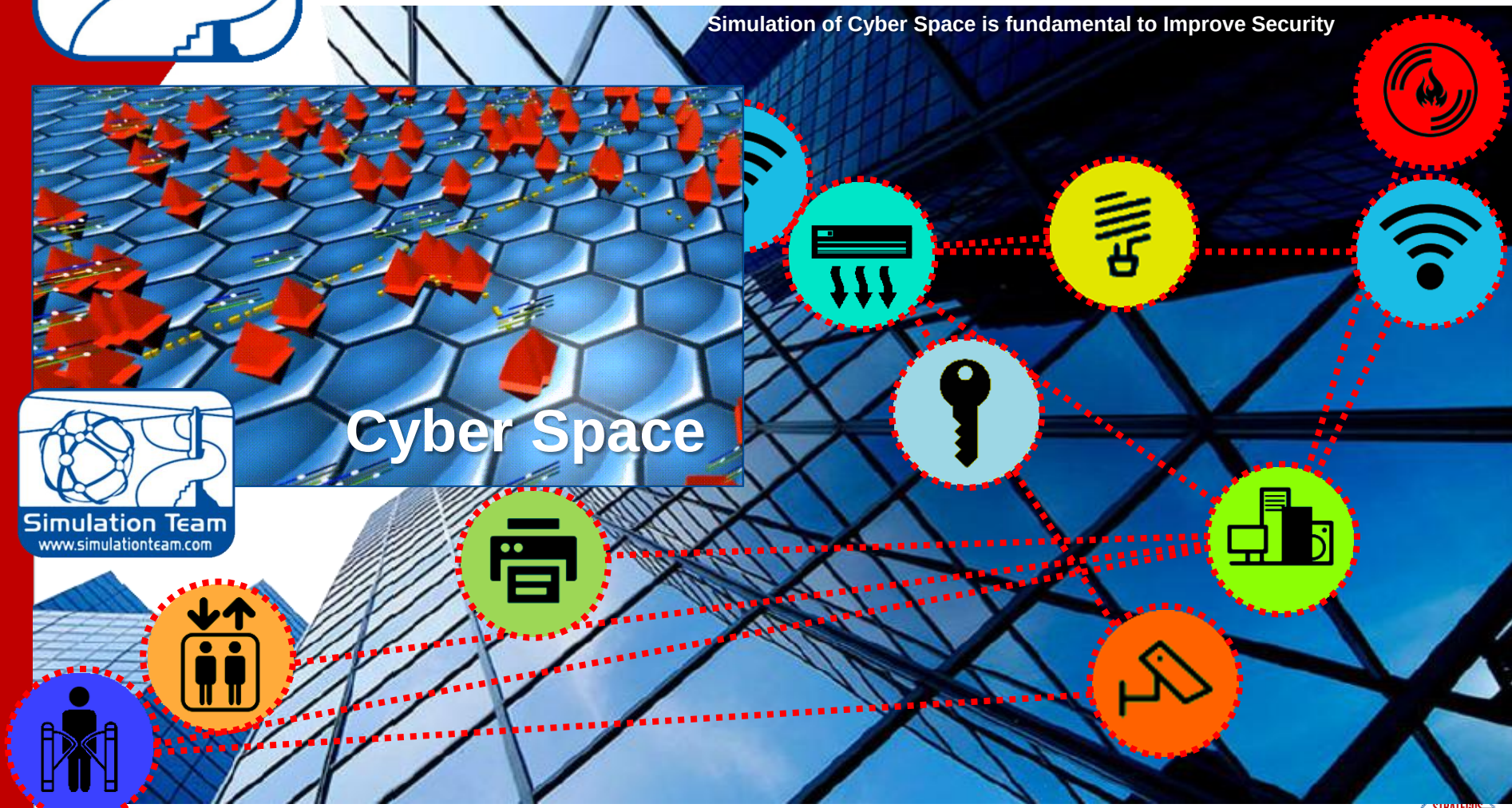
Seeing through Walls



Buildings & Plants
are plenty of devices
that live concurrently
in Physical World
and Cyber Space

...Prevention by Simulation

Simulation of Cyber Space is fundamental to Improve Security

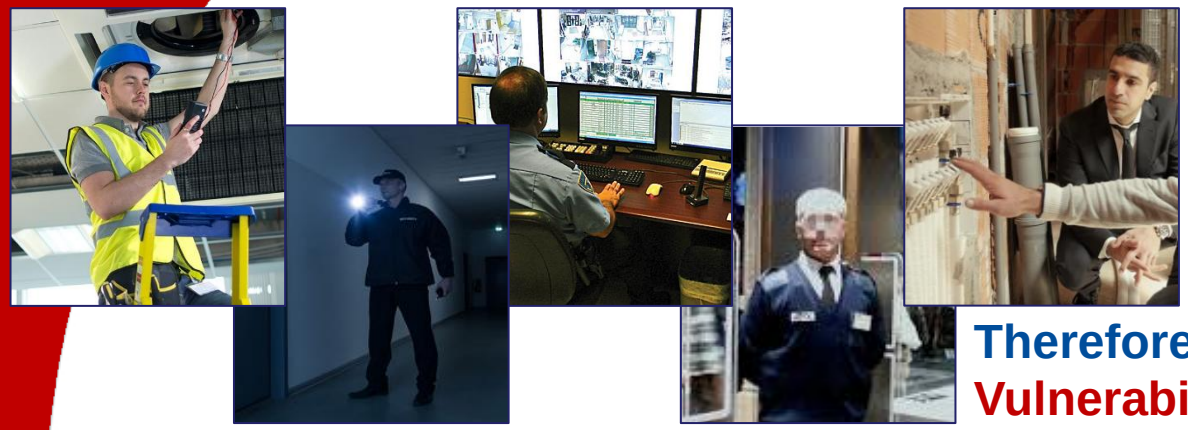


Simulation Team

who watches the watchmen?

Quis custodiet ipsos custodes?

Juvenal, Satires, 347-348



New Technologies are too much convenient to be neglected or even to consider to return back to old solutions

Therefore, New Solutions introduce Vulnerabilities to be addressed

Reduced Personnel, Centralized Supervision, Quick Response, Real Time Monitoring, Distributed Control, Improved Efficiency, 24/7 Support, Big Data for Improving,…

Virtual Assistants based on ICT & IoT

Simulation Team

Computers are more efficient than human beings, not better

Spock, Ultimate Computer

Smart Systems based on AI (Artificial Intelligence) and IA (Intelligent Agents) could improve resilience and defensive capabilities

Therefore, future AI, could have Different Perception and Priorities!

AI could adopt measures that could be affecting Safety and Security. Their evolution Is inevitable, but It requires attention

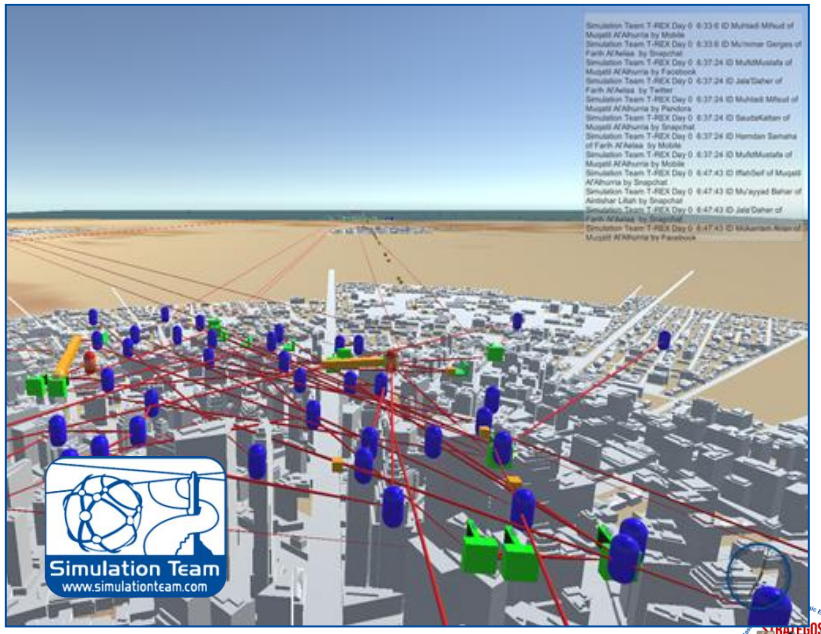
AI, Artificial Intelligence, could Help…
Therefore they could turn in next Threat

Simulation Team

De Docta Ignorantia… Periculi et Ingenio Simulatoris

The idea to reduce risk by limitation on use and diffusion of IoT results hard due to the Costs and Benefits used by this approach
The idea to add protections is for sure necessary, but it is evident that in Cat-and-Mouse Game Attackers keep an advantage position

To be conscious of the Risks and quantify them is crucial
To Plan Preventive Measures, Mitigation Actions & Reactions is fundamentals
The key point is to use MultiLayer Engineering Approach and Simulation to Reduce Vulnerabilities and guarantee Improvements



DMZ Demilitarized Zone
ICCP Inter Chassis Control Protocol

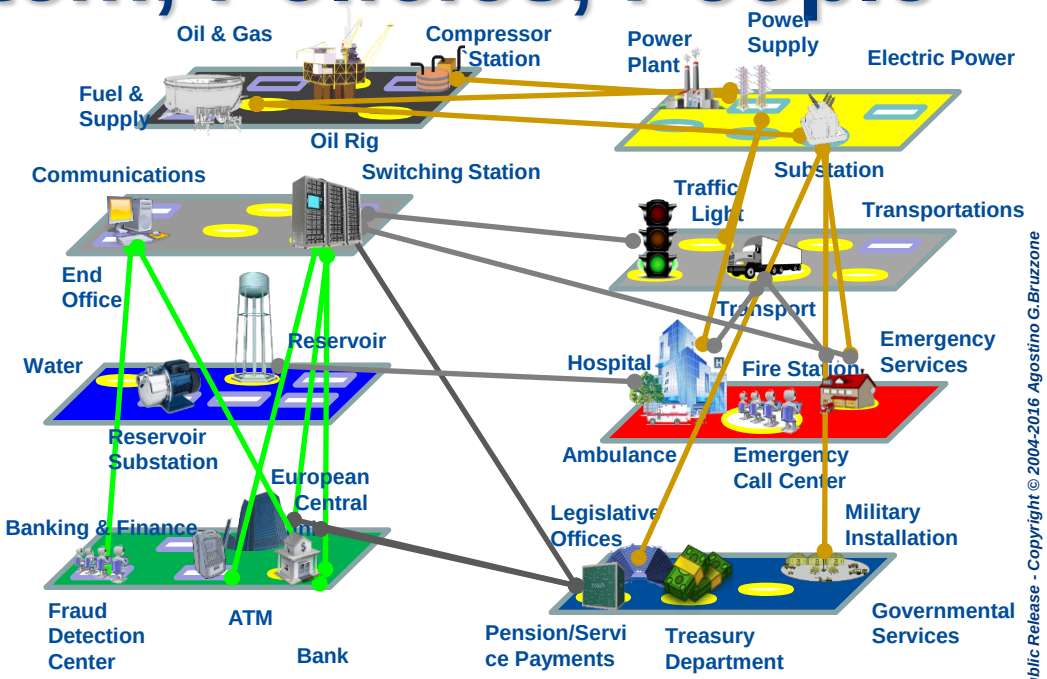
Simulation Team

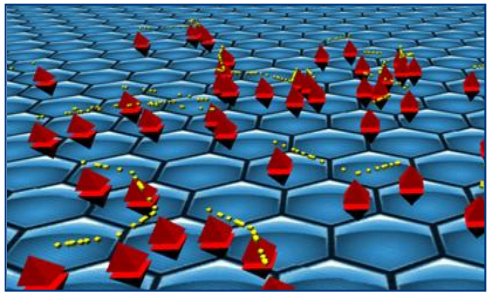
Multi-Layer Simulation for New System, Policies, People

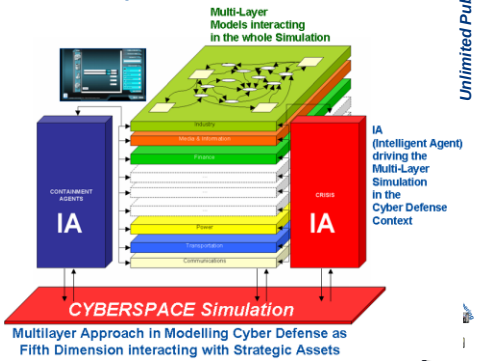
The Modern Systems are usually addressing Multiple Layers and requires to consider multiple aspects for developing

- New System Design
- New Policies & Procedures
- New Technologies and Processes
- Table Top Exercise in order to understand and raise awareness by Human and Machine Learning
- Education & Training Programs for Multiple Players

The use of AI & Intelligent Agent is crucial to automate Smart Simulation



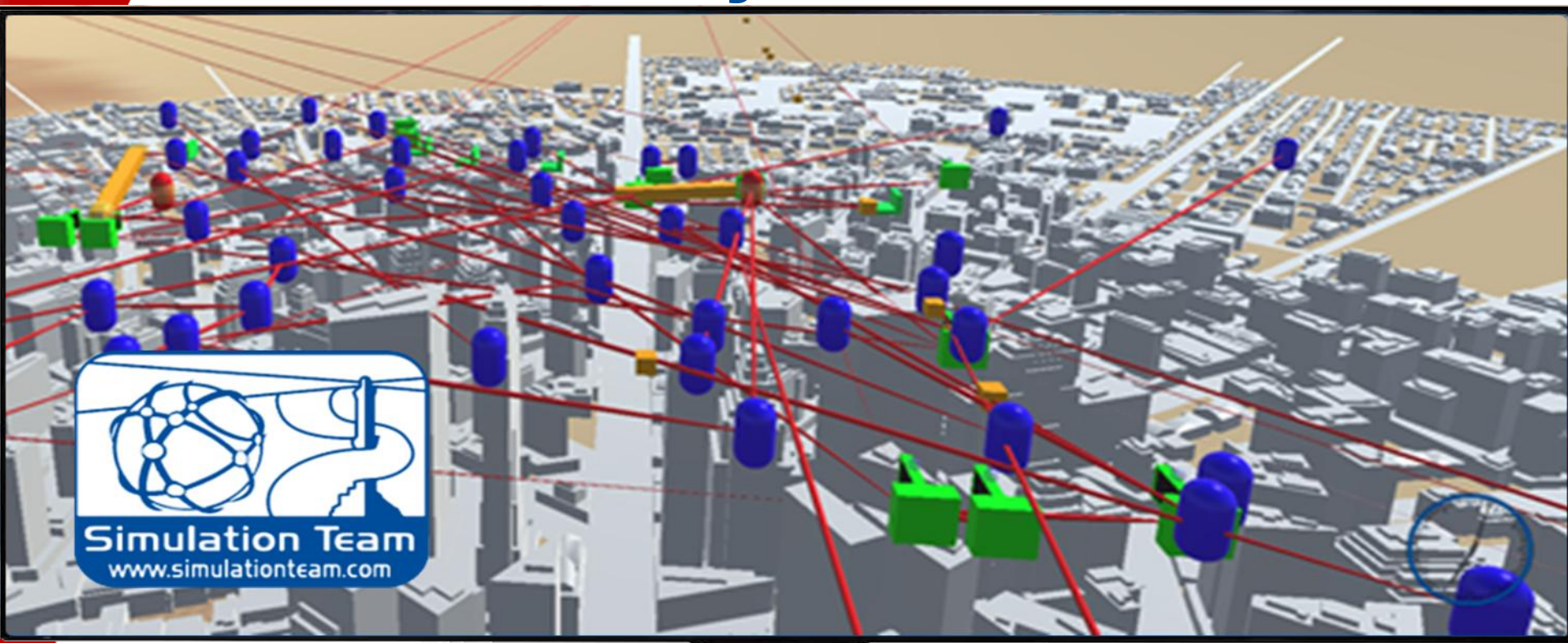




Simulation Team

New Paradigms are emerging… Hybrid Warfare is just one!

We Rebuild the Bridge! Go Great Genoa!
LIBERTAS
Che l'inse?

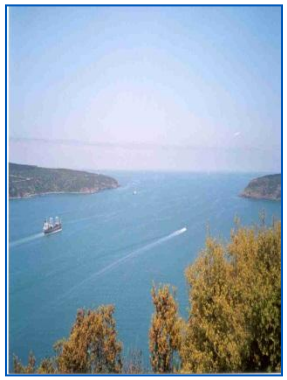


Summarizing

- The use of Strategic Engineering allows a better support to decision making, planning and management within Cyber Warfare, improving quality and reducing vulnerability by consdering their impact on Infrastructures and Real Assets

- The examples confirm the vulnerabilities and the efforts in this sector to develop new apporaches to improve resilience, awareness and responsiveness to protect Organizations, Companies, Society and Critical Infrastructures of a Country

- Simulation, Artificial Intelligence and Data Analytics are key enablers in this area
- The Strategic Engineering approach allows to develop new Decision Support Systems and new Capabilities in Cyber Warfare & Cyber Security



Simulation Team

Prof. Agostino G. Bruzzone

Director of M&S Net (34 Centers WorldWide)
Director of the McLeod Institute Genoa Center
President Simulation Team (26 Partners)
President of Liophant
Council Chair of STRATEGOS
Director Int.Master MIPET

Full Professor in
DIME University of Genoa

via Opera Pia 15
16145 Genova, Italy

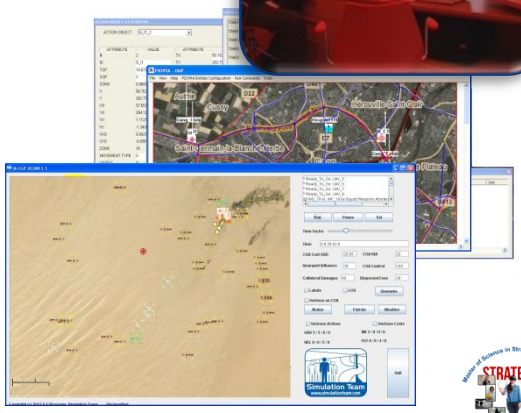
Email agostino@itim.unige.it
URL www.itim.unige.it

DIPTEM

SILENI

MITIM
Simulation Team
Genoa Center

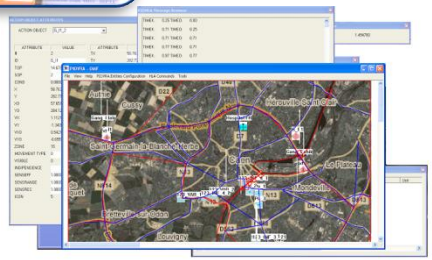
M&SNet



Master of Science in Strategic Engineering
STRATEGOS
www.itim.unige.it/strategos

Simulation Team

References



Simulation Team MITIM
DIME Genoa University
via Opera Pia 15
16145 Genova, Italy
www.itim.unige.it
Agostino G. BRUZZONE
agostino@itim.unige.it

DIME