EXPO 2020 DUBAI UAE

ITALIA
LA BELLEZZA UNISCE LE PERSONE
BEAUTY CONNECTS PEOPLE
الجمال يجمع الناس

OFFICIAL PARTICIPANT – ITALY

Co-Creation LAB

Cyber Critical Infrastructures for Global Supply Chains:
Assets, state of play, threats, attacks, and countermeasures
13th January 2022, 3PM

Abstract

The recent hiccups in the logistic of Global Supply Chains, resulting from the stress posed by the measures to curb the spreading of pandemic, followed by a subsequent acceleration in the world economy, have clearly shown that the global supply chains are inherently fragile. In addition, the same has been seen, to a smaller scale, with the recent cyber-attacks: Colonial Pipeline, that impacted the distribution of oil on the East Coast of the US; Maersk ransomware, whose related outages put a first stress test on the logistics chain; and, solar-winds, whose depth and breadth of compromising (and related consequences) has not been fully understood yet.

In particular, some of the strategic elements that can be identified as critical in global logistic supply chains are the port and airports, as well as the ignitors for the current main sources of energy: Oil and Gas.

The Gulf Countries are, among the other global players, particularly fragile when it comes to the cited Critical Infrastructures, for a number of reasons: the limited number of hubs, the concentration of production of Oil&Gas in specific areas, and the tensions that from time-to-time spur in the area being the main ones.

Given the above scenario, the protection of the cited Cyber Critical Infrastructures: ports, airports, Oil&Gas fields and pipelines, are strategic elements and the very way of living of the Gulf Coast Countries are dependent on.

In this panel, we will discuss the cybersecurity threats, current issues, and possible countermeasures related to the cited domains. In detail, the discussion will touch, but it will not be limited to, the following themes:

- **Maritime Cybersecurity;**
- **Avionics Cybersecurity;**
- **SATCOM security;**
- **Drones as both attack vectors and security enablers.**

Venue   **Accademia** - Italy Pavilion   **Panel Duration** 1h and 10 minutes + 15 minutes Q&A

Agenda   **WELCOME ADDRESS**
Prof. Paola Severino (online) – *VP Luiss University, Rome -Italy*

MODERATORS
Dr. Paolo Spagnoletti, *Luiss University, Rome – Italy*
Mr. Enrico Fazio, *CY4GATE, Rome – Italy*

PANELISTS
Prof. Marc Dacier
Resilient Computing and Cybersecurity Center, King Abdullah University of Science and Technology, Thuwal - Saudi Arabia
Prof. Ernesto Damiani
Director, Center for Cyber Physical Systems, Khalifa University, Abu Dhabi - UAE
Prof. Roberto Di Pietro
College of Science and Engineering, Cybersecurity Research and Innovation Lab, Hamad Bin Khalifa University - Doha - Qatar
Prof. Giuseppe F. Italiano (online)
Director Master Cybersecurity, Luiss University – Rome - Italy
Prof. Maurizio Mensi (online)
Executive Director MENA – OECD Training Centre, Caserta - Italy
Dr. Nadia Saad Noori (online)
Center for Integrated Emergency Management (CIEM), University of Agder, Kristiansand-Norway
Dr. Christina Poepper
Head of Cyber Security & Privacy lab, NYU Abu Dhabi - UAE
Mr. Andrea Raffaelli
Chief Technology Officer, CY4GATE, Rome – Italy