Valencia, 6 May 2016

Port of Valencia at the cutting edge of cyber-security with the MEDUSA project

This morning, the Port Authority of Valencia (PAV) facilities played host to the **"Cyber-security in the Supply Chain: New approaches and challenges"** international conference**,** organized as part of the MEDUSA project, co-funded by the European Commission's DG HOME Directorate General through its Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS) programme.

The conference, organized by the PAV, Fundación Valenciaport and Feports, in their role as members of the European Economic Interest Association - EUROPHAR, was inaugurated by the PAV's Director of Security and Environmental Issues, Federico Torres, and by the Director of Fundación Valenciaport, Vicente del Río. During his speech, Federico Torres highlighted the PAV's involvement in a number of different security projects, as well as implementing groundbreaking initiatives such as CSI (Container Security Management), MEGAPORTS and the ISO 28000 certification. As for Vicente del Río, he pointed out that Fundación Valenciaport, as a member of EUROPHAR, is very much aware of the importance of security, both physical and cyber, within the port logistics chain, to ensure the efficiency and competitiveness of the national economies. It is for this reason that Fundación Valenciaport takes part in European cooperation initiatives, such as the MEDUSA project.

Afterwards, Christos Douligeris, lecturer at the University of Piraeus, presented the main outcomes of the MEDUSA project:

- a risk-assessment tool that deals with the information and communication infrastructures within the supply chain
- a series of prevention and response measures upon detection of a threat at any of the nodes along the supply chain
- a definition of the main scenarios in order to assess the tool, based on container, vehicle and LNG transport.

The conference continued with presentations by Fernando Seco, Director and Consultant at S2 Grupo, who gave a speech about cyber-security on the supply chain, and Rafael Pedrera, Director of Operations at the Cyber Coordination Office of the National Centre for Critical Infrastructure Protection (CNPIC) together with his colleague, Alfonso Ruiz, who spoke about the protection of critical port infrastructures.

Manuel Esteve, Director of the UPV's Distributed Real-Time Systems Lab, then went on to present an integrated control and command management system by applying new display technology to show both the real environment and cyberspace.

This was followed by Pablo Noval, Technical Director of Saggas, who described the flow of the liquefied natural gas (LNG) transport chain, outlining the different actors involved in the supply chain.

The risks and challenges facing the container-transport logistics chain were dealt with by José Gisbert, Head of IT at MSC Terminal Valencia. Gisbert set out the relationships that a container terminal maintains with agents outside the supply chain, the rules and regulations to follow to guarantee security, the main risks and threats they are susceptible to, and what actions should be taken to mitigate them.

During the demo session, Spyros Papastergiou, from the University of Piraeus' Research Centre presented the "MEDUSA Toolkit", a tool designed and developed as part of the project that facilitates an exhaustive analysis of the risks and threats, both physical and cyber, taking into account the "cascading effect" of the entire transportation process by identifying all the data exchange flows between the numerous communication systems involved.

Stefan Schauer, from the Department of Digital Safety and Security at the Austrian Technology Institute then presented MITIGATE, a project sponsored by the H2020 programme with the aim of creating a system that can warn of any cyber risk, allocating a level of importance, as well as a prevention and response measure plan.

The conference culminated with a round table session where participants were available to answer any questions.

The primary aim of MEDUSA, a project that got underway in July 2014 and is expected to be completed in July 2016, is to design risk assessment methodologies for Critical Information Infrastructures that address the different "cascading" effects associated with security incidents that stem from interactions between entities along the supply chain at multiple levels (infrastructural, national, intrasectoral, etc.).