



Cyber-MAR Vessel Pilot

Vessel Cyber Attack in Port of Valencia

5th May 2022

Introduction to Port of Valencia

The port of Valencia is a major European port, handling over 6 million tonnes of cargo a year. The port also serves as an important regional hub, handling a large number of the imports, exports and transshipments that take place in the region.

The port handles a wide variety of cargo including liquid bulk, dry bulk, containerised cargo and vehicular traffic. In addition to this, the port also hosts a number of passenger ships each year, including cruise ships. Due to the importance of this port to the European economy, it is of utmost importance to EU trade.



Port Of Valencia

The vessel scenario that is considered in today's pilot constitutes a scenario where an attacker launches an attack that allows them to temporarily alter the course of a large container vessel and in so doing cause a blockage on the approach channel.

Progression of Attack can be broken down into a number of stages:

- Downloading and Propagation of Attack (Within IT Infrastructure)
- Installing and Initiating the Attack on Vessel Control Systems
- Attack realisation and crew response

Setting the Scene - Introduction of Ship Model

Large Container Vessel

Length	397 m (1,302 ft 6 in)
Beam	56 m (183 ft 9 in)
Draught	16.02 m (52 ft 7 in)
Depth	30 m (98 ft 5 in) (deck edge to keel)
Speed	25.5 knots (47.2 km/h; 29.3 mph)
Capacity	•14,770+ TEU





 www.Cyber-MAR.eu

 [Cyber_MAR](https://twitter.com/Cyber_MAR)

 [Cyber-MAR EU Project](https://www.youtube.com/Cyber-MAR)

 [Cyber-MAR](https://www.linkedin.com/company/Cyber-MAR)

 info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION



This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement No. 833389