Evaluation of monetary impacts of cyber-attacks on global supply chains in ports

Purpose:

This paper presents, what kind of impacts different types of cyber-attacks have in port environment, and aims to evaluate economic losses of various types of disruptions in port environment. Based on the information about monetary losses of possible cyber-attacks, the organizations have better possibilities to estimate the value of investments for preventing those attacks.

Methodology:

This paper applies developed econometric model, which has the capability of quantifying the indirect economic impact of port disruptions caused by cyber-attacks on global supply chains. The used quantitative risk model emulates major components of global supply chains and their uncertainties to estimate the economic losses resulting from contingent business interruption caused by disruptions to a given supply chain node – in this case, disruptions to ports.

Findings:

The demand for high-level resilience in global maritime supply chains, in addition to better business continuity management, is becoming increasingly important as global markets seek rapid responses to change. Based on used econometric model, even small disruptions in a port can cause significant monetary losses and problems in supply chains.

Originality:

This paper contributes on supply chain resilience literature by evaluating indirect impacts on cyber-attacks on global supply chain by focusing on port environment.

Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389.