Contribution ID: **117** Type: **Paper**

Naval automation cyber defence guidelines

Friday, 22 June 2018 12:15 (15 minutes)

It’s been 15 years since “cyber risk” was identified as the new millennium threat, potentially affecting organizations, industries, governments and society. Despite choral worries, the naval context has seemed to remain unaffected for years, as long as ships could have been considered “isolated systems” floating offshore. But, as new technologies (either commercial or military) had spread out on in this rapidly becoming “information-dependent” and “inter-connected” shipping industry, cyber risk finally become a threat . As the matter turned into business, many solutions have been developed in order to grant cyber-security, at user level (i.e.: personal, office, enterprise, server farm..). Could these solutions completely protect a ship themselves? How much a shipowner has to invest in cyber-security? How he could efficiently face cyber-threat? This kind of questions generally have no straight answer because nobody can find a proper solution without an assessment, tailored on the specific case of context. This work is intended to advise ship owners on the importance of an effective cyber-risk assessment before the choose of a cyber-security solution and, in the meantime, it suggests an easy way to conduct it, formulated on the basis of classical risk-assessment procedures.

Primary author: Mr CARDELLICCHIO, Davide (Marina Militare Italiana)

Presenter: Mr CARDELLICCHIO, Davide (Marina Militare Italiana)

Session Classification: Navy and Cyber Security

Track Classification: Naval ships design & technology