ECSA
European Community Shipowners' Associations

POSITION PAPER
TBC/November 2023

CYBER SECURITY FOR SHIPS : DRAFT ECSA POLICY POSITION PAPER

Introduction

Cyber-security incidents can cause high disruption to shipping companies of all sizes. As such, shipping companies take such risks seriously and international regulations already require cyber-risk management for ships.

The existing international regulations are important to ensure cyber risk-management measures are in place and specific to diverse types and functions of internationally-trading ships. There are also commercial incentives ensuring ships implement cyber-risk management, together with industry best-practice guidelines. A description of these existing measures is below, followed by possible ways in which EU-policy could further enhance cyber-security for European shipping.

In addition, existing EU requirements should take into account the NIST cybersecurity framework.

Existing requirements and drivers to cyber-risk management for ships

- **ISM**: Shipping companies have since 1 January 2021[1] been obliged to ensure that cyber risks to ships are appropriately addressed in Safety Management Systems to comply with the International Safety Management (ISM) Code. This follows an IMO Resolution and corresponding cyber risk management Guidance recommending shipping companies to identify and protect against cyber risks and develop ways to respond and recover from them. The guidelines recognise that '*no two organizations in the shipping industry are the same'* with the recommendations expressed in broad terms in order to have a widespread application. Since the requirements have been introduced, shipping companies report a heightened overall awareness of cyber-risks throughout their organisation. The ISM Code is implemented at EU level by EC 336/2006.
- **ISPS**: The International Ship and Port Facility Security (ISPS) Code requires i.a. that shipping companies conduct overall security risk assessments and plans for approval by the Flag State. This code is implemented at EU level by EC 725/2004, which makes mandatory some of the Code's 'Part B' which is otherwise voluntary. It specifies that ship security assessments should also address radio and telecommunication systems including computer systems and networks and possible vulnerabilities in communication systems. These requirements can be addressed as a part of the cyber risk management in the Safety Management System with a reference in the ship security assessment.
- **Unified Requirements adopted by the International Association of Classification Societies (IACS) (UR-E 26 & EUR 27)** : this standards are related to new builds and new equipement and provide cybersecurity "by design" requirements (applicable to

[1] Or no later than Document of Compliance annual verification

ECSA is a trade association representing the national shipowners' associations of the EU and Norway. The European shipowners control 40% of the global commercial fleet. ECSA promotes the interests of European shipping so that the industry can best serve European and international trade in a competitive free business environment to the benefit of shippers and consumers.

vzw ECSA asbl, Boulevard du Régent, Regentlaan 43-44, 1000 Brussels, Belgium
T +32 2 510 61 20 • mail@ecsa.eu • www.ecsa.eu

new ships contracted for construction on and after 1 July 2024)

- **Industry best practice guidance**: Shipping industry groups have developed specific guidance to support shipping companies identify and manage cyber risks. The Guidelines on Cyber Security Onboard Ships are now in their fourth version.
- **Commercial incentives**: Vetting programmes are in place for shipping companies to demonstrate to charterers and cargo owners that cyber risk-management is implemented onboard ships. An example is the Tanker Management and Self-Assessment. Several classification societies also offer specific class notations as a mark of cyber resilience.

ECSA considerations for EU policy

At the EU level, the above regulations and other drivers are supplemented by the NIS 2 Directive which supports a wider culture of cyber security and preparedness across the Union member states and economic sectors. For European shipping it is however important that the scope this EU Directive continues to give preference to the *international* cyber regulations applicable to individual ships. These provide the needed flexibility for shipping companies to adapt measures to the specifics of their fleet while reducing the administrative costs of compliance for ships that are constantly transiting different jurisdictions. Looking ahead, ECSA considers several ways EU policy-making can enhance cyber-security for shipping :

- **Encouraging the *voluntary* reporting of ship cyber incidents to Flag States in a more harmonised way:** Improved reporting and analysis of cyber incidents faced to ships could help develop a better picture of the actual nature and severity of the risks. Such information could, in turn, better inform the safety and security management plans the international regulations require. Although shipping companies already have obligations to report safety issues occurring onboard to the Flag State (which should remain the primary channel of such communication) the reporting of cyber incidents could be further encouraged if that's not already the case due to Flag-specific requirements. This encouragement could include, for example, assurance that reports of cyber-incidents will remain confidential, nor penalise the shipping company for doing so. Some non-mandatory recommendations towards a more harmonised way of reporting cyber incidents onboard ships could potentially support the better identification of cyber risk patterns (i.e. location of incidents, threat type, possible source of incidents). These reports, kept confidential and secure, could be anonymised and used towards the publication of i.e. government-issued maritime cyber threat assessments, for example.
- **Raising awareness of 'cyber-hygiene' across all industries:** The shipping sector is the conveyor of global trade carrying 90% of all goods and is an interconnector to many different economic actors and activities. In this regard, an overall heightened awareness of cyber security across supply chains and the industries that shipping serves is important. EU non-binding publications such as the 'transport toolkit' and key messages issued in December 2020 are useful to support 'cyber hygiene' across all transport modes. Further simple, short recommendations could in particular be encouraged i.e. on the effective control and verification of emails of IT systems used onboard. Ships also receive numerous external personnel onboard around the world (surveyors, pilots, etc), to whom access to OT and IT systems onboard could be restricted.
- **Cyber-security in the training of crew:** As technological developments

in the shipping industry will continuously evolve, more attention to cyber-security could be considered with respect to any future STCW review at IMO level.