Shipping Italy
Il quotidiano online del trasporto marittimo

Focus di Enrico Vergani su responsabilità, assicurabilità e gestione del rischio cyber dopo l'attacco a Gnv

Nicola Capuzzo · Friday, December 19th, 2025

Il caso del traghetto Gnv Fantastic, fermato nel porto di Sète e coinvolto in un'indagine per un presunto tentativo di compromissione informatica, ha attirato l'attenzione dell'opinione pubblica e del settore marittimo. Al di là degli sviluppi giudiziari, l'episodio ha sollevato interrogativi più ampi su responsabilità, assicurabilità e gestione del rischio cyber nel trasporto marittimo.

SHIPPING ITALY ha approfondito l'argomento con l'avvocato Enrico Vergani, partner dello studio legale internazionale Campbell Johnston Clark, uno dei maggiori esperti italiani di diritto marittimo e assicurativo.

Avv. Vergani, cosa rende il caso Gnv Fantastic giuridicamente rilevante, al di là del singolo episodio?

"Il punto centrale non è tanto il fatto in sé, quanto ciò che esso rappresenta. Il caso Fantastic mette in evidenza come eventi cyber, anche quando non producono danni immediati, possano generare conseguenze giuridiche complesse se inseriti in un contesto ibrido, tra criminalità, sicurezza e competizione tra Stati."

In che modo la qualificazione giuridica dell'evento incide sulle responsabilità?

"In scenari di questo tipo, la qualificazione ex post dell'evento è determinante. Stabilire se si tratti di atto di guerra, terrorismo, sabotaggio o criminalità comune non è affatto immediato. E ogni qualificazione attiva regimi di responsabilità profondamente diversi, con impatti diretti sull'armatore, sul Comandante e sugli altri soggetti coinvolti."

Questo vale anche in assenza di danni materiali o lesioni?

"Assolutamente sì. Anche senza un danno concreto, la sola esposizione a un rischio cyber può aprire interrogativi su organizzazione, procedure e adeguatezza dei sistemi adottati. È per questo che questi eventi meritano un'analisi giuridica sin dalle prime fasi."

?Il tema cyber si collega a concetti classici del diritto marittimo?

"Ormai in modo strutturale. Penso in particolare alla seaworthiness e alla due diligence

dell'armatore. Un malfunzionamento dei sistemi critici di bordo — navigazione, propulsione, comunicazioni — dovuto a vulnerabilità note o che avrebbero dovuto essere note, a una gestione inadeguata degli accessi o a patching insufficiente, può essere letto come una carenza organizzativa e procedurale, non solo tecnica."

Esiste un quadro normativo chiaro su questi aspetti?

"Il quadro esiste ed è in continua evoluzione. A livello internazionale, la risoluzione Imo Msc.428(98) ha esteso di fatto il Codice Ism alla gestione del rischio cyber, rendendola parte integrante della sicurezza operativa. In ambito europeo, la direttiva Nis2 amplia ulteriormente gli obblighi di cybersecurity per gli operatori marittimi critici."

Come reagisce il mercato assicurativo di fronte a questi scenari?

"Con crescente attenzione, ma anche con molte cautele. Il problema non è tanto una mancanza assoluta di copertura, quanto un disallineamento tra la natura del sinistro cyber e l'architettura delle polizze marittime tradizionali."

Dove si concentrano le principali aree di frizione assicurativa?

"Nelle esclusioni. Nelle polizze Hull & Machinery, clausole come la CL.380 escludono perdite causate dall'uso dei sistemi informatici "come mezzo per infliggere danno". Endorsement come Lma5403 cercano di ridurre l'ambiguità, ma lasciano comunque aree grigie, soprattutto quando è difficile distinguere tra attacco intenzionale, sabotaggio o semplice system failure."

E sul fronte P&I e polizze cyber standalone?

"Le difficoltà aumentano quando l'evento viene ricondotto a war risks o a operazioni attribuibili a Stati. In questi casi entrano in gioco esclusioni per guerra, ostilità o atti "state-backed", con il rischio concreto di contestazioni sulla copertura proprio nei casi più gravi."

Questo significa che una parte rilevante del rischio potrebbe restare scoperta?

"È una possibilità concreta. Studi recenti indicano che una percentuale molto elevata dei costi derivanti da un grave incidente cyber nel settore marittimo potrebbe non essere coperta. Per questo la gestione del rischio cyber sta diventando, di fatto, una condizione di assicurabilità."

Qual è allora il vero cambio di paradigma richiesto allo shipping?

"La consapevolezza. La gestione del cyber risk deve salire al livello più alto della governance aziendale, con un approccio olistico che integri aspetti tecnici, organizzativi, legali e assicurativi. Le coperture assicurative dovrebbero intervenire solo dopo che tutto ciò che era ragionevolmente possibile fare internamente è stato fatto."

In chiusura, una domanda più personale: cosa la tiene sveglio la notte, quando pensa al futuro del settore marittimo e al rischio cyber?

"Il fatto che, nonostante segnali sempre più evidenti, una parte del settore continui a percepire il rischio cyber come astratto o remoto. Il vero pericolo non è l'attacco in sé, ma arrivare impreparati, scoprendo troppo tardi che responsabilità, coperture e aspettative non erano allineate alla realtà."

> Cyber a bordo: il caso Fantastic e le aree di rischio ancora poco esplorate nel settore marittimo

> 'Giallo' cyber a bordo del traghetto Fantastic di Gnv

This entry was posted on Friday, December 19th, 2025 at 11:05 am and is filed under Interviste
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.