Shipping Italy
Il quotidiano online del trasporto marittimo

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

Nicola Capuzzo · Friday, December 19th, 2025

*Contributo a cura di Mark William Lowe **

** Director Monact Risk Assessment Services*

Il caso del traghetto *Fantastic* di GNV, fermato nel porto di Sète e coinvolto in un'indagine per un presunto tentativo di compromissione informatica scoperto e segnalato alle autorità competenti dalla compagnia di navigazione, potrebbe essere liquidato come un episodio isolato, dai contorni ancora poco chiari.

Tuttavia, osservato nel contesto più ampio della sicurezza marittima e delle attuali dinamiche geopolitiche, l'episodio solleva interrogativi che vanno ben oltre il singolo evento. Non si tratta di affermare che le navi siano oggi facilmente controllabili dall'esterno, né di suggerire falle sistemiche nella sicurezza del settore. Piuttosto, emerge il rischio che alcune tipologie di minaccia non siano ancora pienamente comprese, soprattutto quando si collocano in una zona grigia tra criminalità, sicurezza e competizione tra Stati.

Chi ha pagato l'equipaggio: una possibile logica di osservazione

Secondo un ex ufficiale d'intelligence con una profonda conoscenza delle modalità operative russe nel dominio ibrido, lo scenario del *Fantastic* appare coerente con schemi già osservati in Europa negli ultimi anni.

"Per il momento," osserva, "lo scenario sembra compatibile con una serie di azioni di *grey zone hybrid warfare* che la Russia porta avanti da tempo in diversi Paesi europei."

In questa prospettiva, l'obiettivo non sarebbe necessariamente causare danni immediati o prendere il controllo della nave.

"Queste operazioni," spiega, "sono spesso progettate per testare vulnerabilità, valutare se tentativi simili potrebbero funzionare e stabilire se una determinata tecnica sia già efficace o debba essere affinata."

Si tratterebbe quindi, in molti casi, di vere e proprie operazioni di intelligence.

“Sono attività di *stress testing*,” prosegue, “che servono anche a raccogliere informazioni fondamentali su come reagiscono i diversi attori coinvolti.”

Gli attori osservati non sarebbero solo armatori e autorità portuali.

“I soggetti sotto osservazione includono anche i servizi di sicurezza e di intelligence degli Stati, i governi interessati e, non da ultimo, l’opinione pubblica.”

In questo quadro rientrano anche le preoccupazioni del mondo del lavoro marittimo.

“Non si possono ignorare le reazioni dei sindacati e delle associazioni dei lavoratori del settore, così come la percezione dei passeggeri. Una delle domande chiave è se episodi di questo tipo possano generare timori tali da influenzare la propensione a viaggiare.”

Secondo la fonte, il fatto che il caso sia rimasto relativamente sotto traccia non ne riduce la rilevanza.

“Questo episodio sembra mantenere un profilo basso, ma chi ne è a conoscenza è tutt’altro che tranquillo.”

Un elemento ricorrente in questo tipo di operazioni è la difficoltà di attribuzione.

“Quando Mosca intende condurre uno stress test,” spiega l’ex ufficiale, “non ha alcuna difficoltà a nascondere la propria mano, costruendo quella che in inglese chiamiamo *plausible deniability*: operazioni organizzate in modo da non poter essere ricondotte a un mandante ultimo.”

La catena operativa è spesso indiretta.

“Attraverso una serie di intermediari,” aggiunge, “non è mai un problema individuare chi, per qualche migliaio di euro, è disposto ad agire per conto terzi.”

Si tratta, nella maggior parte dei casi, di soggetti marginali.

“Parliamo spesso di criminali di basso livello, con pochi scrupoli, pronti a incendiare un deposito, introdurre un pacco su un aereo o far arrivare apparecchiature tecnologiche su una nave.”

La consapevolezza dell’operazione è limitata.

“Molto spesso queste persone non hanno idea di ciò che stanno realmente facendo né di chi ci sia dietro. Se sospettano un collegamento con Mosca, alcuni vivono la cosa come eccitante, quasi fosse un gioco da film; altri simpatizzano apertamente; altri ancora semplicemente non si pongono il problema.”

La leva economica resta decisiva.

“Per questo tipo di individui,” conclude, “qualche migliaio di euro rappresenta una somma significativa. E, realisticamente, qualcuno disposto a farlo si trova sempre.”

La tecnologia: ciò che non sappiamo e ciò che non si può escludere

Al momento non è noto quale tecnologia fosse effettivamente in possesso degli indagati, né quali fossero le loro reali intenzioni operative. È generalmente riconosciuto che una presa di controllo remota dei sistemi di navigazione o di propulsione da grande distanza sia altamente improbabile.

Tuttavia, se un soggetto presente a bordo riuscisse a infiltrare i sistemi informativi della nave, non si può escludere il rischio di una temporanea perdita o degradazione di alcune funzioni operative. Non si tratta di una vulnerabilità strutturale delle navi, ma della combinazione tra accesso fisico, conoscenze tecniche e procedure non ottimali.

Sistemi progettati per la resilienza, ma attenzione al contesto operativo

Le navi moderne sono progettate per essere resilienti, con sistemi ridondanti e procedure manuali. Tuttavia, l'efficacia di tali misure dipende anche dal contesto operativo: manutenzione, aggiornamenti software, operazioni portuali, interventi di terze parti.

Il rischio è che l'attenzione si concentri eccessivamente sugli aspetti tecnici, trascurando la dimensione organizzativa e procedurale. Il tema non è la perdita totale di controllo, ma la possibile degradazione parziale delle capacità operative in momenti critici.

Implicazioni legali: quando il rischio diventa responsabilità

Nel caso in cui un evento di questo tipo dovesse causare danni materiali o lesioni a persone, le conseguenze legali potrebbero essere particolarmente complesse.

"In scenari di questo genere," osserva Enrico Vergani, Partner dello studio internazionale Campbell Johnston Clark, "la questione centrale non è solo l'evento in sé, ma la sua qualificazione giuridica *ex post*."

La distinzione tra atto di guerra, terrorismo, sabotaggio o criminalità comune non è immediata, soprattutto in presenza di elementi riconducibili a operazioni ibride.

"Ogni possibile qualificazione," prosegue Vergani, "attiva regimi di responsabilità profondamente diversi e può incidere in modo significativo sulla posizione dell'armatore, del Comandante e degli altri soggetti coinvolti."

Assicurazione e rischio di contenzioso

Dal punto di vista assicurativo, questi scenari aprono aree di incertezza non trascurabili.

"Il rischio cyber," sottolinea Vergani, "si intreccia ormai con concetti cardine del diritto marittimo come la *seaworthiness* e la *due diligence*."

Un malfunzionamento dei sistemi critici di bordo causato da vulnerabilità note, o che avrebbero dovuto essere note, può essere interpretato come una carenza organizzativa e procedurale, non solo tecnica.

"Questo ha un impatto diretto sull'assicurabilità del rischio," spiega. "In caso di sinistro, l'attenzione dell'assicuratore non si concentrerà solo sull'attacco, ma anche su ciò che l'armatore ha fatto — o non ha fatto — prima."

Le polizze Hull & Machinery, così come le coperture P&I, presentano spesso esclusioni legate a

cyber risk, war risk o atti attribuibili a Stati.

“Non è tanto una mancanza di assicurazione,” chiarisce Vergani, “quanto un disallineamento tra la natura del sinistro e l’architettura delle polizze. Questo può tradursi in aree grigie e in contenziosi complessi sulla copertura.”

Anche le polizze cyber standalone non eliminano del tutto il problema, soprattutto in presenza di clausole di esclusione per eventi statuali o assimilabili a operazioni di guerra.

Una riflessione più ampia

Il caso *Fantastic* non dimostra l’esistenza di una minaccia imminente o sistemica. Tuttavia, evidenzia come alcune aree di rischio — dove tecnologia, fattore umano, diritto, assicurazione e geopolitica si sovrappongono — siano ancora insufficientemente esplorate.

In un settore che gestisce volumi, valori e responsabilità enormi, una riflessione aperta e non difensiva su questi temi non indebolisce il trasporto marittimo. Al contrario, ne rafforza la resilienza, la credibilità e la capacità di affrontare un contesto di rischio sempre più complesso.

ISCRIVITI ALLA NEWSLETTER QUOTIDIANA GRATUITA DI SHIPPING ITALY

SHIPPING ITALY E’ ANCHE SU WHATSAPP: BASTA CLICCARE QUI PER ISCRIVERSI AL CANALE ED ESSERE SEMPRE AGGIORNATI

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

> ‘Giallo’ cyber a bordo del traghetto Fantastic di Gnv

This entry was posted on Friday, December 19th, 2025 at 11:03 am and is filed under Economia
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.