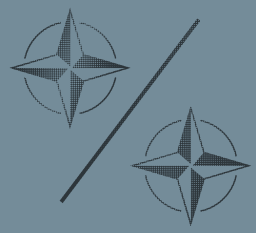
AirPress

Mensile sulle politiche
per l'aerospazio e la difesa

n. 167 - giugno 2025

SPECIALE
NATO SUMMIT

Give me Five!



Giuseppe Cavo Dragone, Alessandro Minuto Rizzo, Valbona Zeneli, Francesco M. Talò, Lorenzo Cesa, Stefania Craxi, Stefano Graziano, Antonino Minardo, Fiona Murray, Pasquale Preziosa, Fabrizio Braghini

Difesa

Spyderweb, una lezione per le operazioni di domani

IVAN CARUSO

Cyber

Tutti i guai del mare digitale

ANNITA LARISSA SCIACOVELLI

Spazio

Dentro lo scontro tra Musk ed Ergen

MARCELLO SPAGNULO

sommario

Airpress
Agenzia stampa aeronautica tecnica politica

Registrazione Tribunale di Roma n. 10311 del 7/4/1965. Registrazione R.O.C. n. 9884

Editore Base per altezza s.r.l.
corso Vittorio Emanuele II, 18 · 00186 Roma

telefono 06 454 73 850 · fax 06 455 41 354
partita iva 05831150966

Rivista fondata da
Fausto Alati

Direttore responsabile
Flavia Giacobbe

Redazione
Riccardo Leoni

Ha partecipato
Jacopo Marzano

Progetto grafico
blueforma

Impaginazione e grafica
Intorno Design

Per comunicati, abbonamenti, pubblicità
airpress@formiche.net

Recapito a cura di Fdc Services srl

Numero chiuso in redazione
il 12 giugno 2025

Finito di stampare
il 15 giugno 2025

Stampato in Italia
da Rubettino print
Viale Rubbettino, 10
88049 Soveria Mannelli

Cyber

Tutti i guai del mare digitale

La crescente digitalizzazione del settore e l'integrazione dell'IA agentica renderanno i sistemi infrastrutturali marittimi ancora più suscettibili a rischi informatici, e le decisioni autonome di sistemi intelligenti, senza supervisione umana, aumenteranno la possibilità di azioni malevoli o errori imprevisti che potrebbero compromettere la sicurezza operativa. La necessità di garantire sistemi di protezione robusti e una resilienza adeguata è ora più urgente che mai

ANNITA LARISSA SCIACOVELLI
Esperta di cybersecurity, docente di Diritto internazionale e membro dell'advisory board di Enisa

Nel mondo marittimo, la trasformazione digitale sta riconfigurando il modo in cui porti, navi e sistemi logistici operano. Tecnologie come *l'Internet of Things* (IoT) e l'intelligenza artificiale se, da un lato, stanno rivoluzionando il funzionamento dei porti rendendoli sempre più intelligenti e di navi autonome, cioè senaza equipaggio, dall'altro lato espongono l'intero ecosistema marittimo a nuovi rischi. In particolare, lo sviluppo dell'intelligenza artificiale agentica, ovvero capace di prendere decisioni autonome, apre scenari inediti e potenzialmente critici per la sicurezza, specialmente quando si parla di sistemi di bordo e operazioni automatizzate. Questa evoluzione tecnologica, che sicuramente comporterà notevoli benefici, si innesta in un quadro di crescenti minacce e rischi. Negli ultimi anni si sono moltiplicati i casi di attacchi mirati a infrastrutture marittime. Ad esempio, a febbraio 2025, i porti di Trieste e Taranto sono stati colpiti da *cyber*-attacchi che hanno compromesso i sistemi Ict. Episodi analoghi si sono verificati in altri Stati europei, come il porto di Ostenda in Belgio. Inoltre, sempre più navi, porti e operatori logistici stanno diventando bersaglio di attacchi sofisticati provenienti da attori o gruppi criminali sponsorizzati da Stati con obiettivi di spionaggio politico o tecnologico, come già evidenziato dall'Agenzia europea per la cyber-security – Enisa, nel "Threat landscape*:* transport sector 2023", che evidenzia come il settore marittimo sia sempre più esposto a minacce digitali sistemiche e caratterizzato da un elevato numero di vulnerabilità. In particolare, le campagne di *phishing* e gli *exploit zero-day* rappresentano minacce e modalità di attacco sempre più utilizzati dai *cyber*-criminali per compromettere i sistemi portuali e le navi. Sempre Enisa nel report "Nis 360" del 2025, evidenzia sia come il settore marittimo per la sua importanza strategica ed economica, rientri nella zona a rischio in materia di sicurezza informatica per l'Unione europea, sia come tale settore si caratterizzi per un significativo divario rispetto al livello di maturità di sicurezza informatica richiesto alle infrastrutture critiche dalla direttiva 2022/2555, nota come direttiva Nis 2. Questo *gap* riguarda la capacità delle infrastrutture marittime di gestire in modo efficace le minacce *cyber*, atteso che la loro continuità operativa è vitale sia per la sicurezza nazionale sia per la competitività dei sistemi portuali a livello internazionale. In realtà, la rapida evoluzione tecnologica aggiunge nuove sfide alle già notevoli complessità della gestione dei servizi infrastrutturali marittimi, finora concentrati sulla sicurezza fisica dei sistemi autonomi.
A tal scopo, l'Unione europea ha recentemente adottato la direttiva (Eu) 2022/2557 sulla resilienza delle entità critiche, nota come direttiva Cer, che dovrà essere applicata entro il 2026 e che disciplina la sicurezza informatica anche delle infrastrutture portuali, richiedendo piani di gestione del rischio, audit e *business continuity*. Nello

Gli effetti del pacchetto Safe sui partner

Con una procedura d'urgenza che ha escluso il Parlamento europeo, il Consiglio dell'Unione ha approvato il regolamento *Security action for Europe* (Safe), superando gli ostacoli politici che ne avevano rallentato l'approvazione. La scelta di ricorrere all'articolo 122 del Trattato ha suscitato critiche e l'Eurocamera valuta un ricorso alla Corte di giustizia. Il nuovo strumento mira a rafforzare la base industriale europea della difesa, introducendo elementi innovativi come l'estensione della partecipazione oltre l'Ue, secondo una logica di "Europa geografica", e condizioni che richiamano forme di preferenza europea già previste da altri regolamenti. I prestiti saranno concessi sulla base di una logica *demand driven*, ovvero su richiesta da parte di almeno due Paesi eleggibili per acquisti comuni (in casi eccezionali anche uno solo), che dovranno trasmettere alla Commissione europea piani di investimento nella difesa (European Defence industry investment plans). L'elenco dei partecipanti potenziali comprende i 27 Stati membri Ue, quelli Eea-Efta, l'Ucraina, i Paesi candidati all'adesione e quelli con accordi di sicurezza e difesa con l'Ue (come il Regno Unito, prossimo firmatario). Sono previste anche intese bi o multilaterali, ma l'unanimità necessaria potrebbe esporle a blocchi politici. I prodotti eleggibili devono avere origine da imprese con quartier generale in Ue/Eea-Efta/Ucraina. Per i beni non complessi o di consumo bellico, il 65% del valore deve derivare da componenti europei. Per i sistemi complessi, sono richieste garanzie di controllo tecnologico, come la titolarità del progetto (System design Authority), per evitare nuove dipendenze extra-Ue. Pur articolato e complesso, Safe consente una certa flessibilità operativa per Stati e Commissione, rafforza le industrie della difesa nei Paesi membri e apre a una *supply chain* più ampia. Se il meccanismo si dimostrerà efficace, potrebbe portare al passo successivo: spostare l'acquisto di capacità militari dalle logiche nazionali a una vera pianificazione europea, con finanziamenti direttamente dal bilancio dell'Ue.

stesso senso, la Strategia per la sicurezza marittima dell'Ue (Eumss), aggiornata nel 2023, sottolinea l'importanza della *cyber-security* come pilastro fondamentale della gestione integrata dello spazio marittimo europeo. A livello internazionale, sul piano tecnico-operativo, l'Organizzazione marittima internazionale (Imo) nel 2022 ha adottato le *Guidelines on maritime cyber risk management* e *le measures to enhance maritime security* che completano il quadro normativo per affrontare le minacce *cyber* in modo strutturato e coordinato. Nel loro insieme, le misure proposte dalla Imo e dalla direttiva Cer forniscono un quadro di riferimento fondamentale per garantire che le operazioni marittime rimangano sicure, nonostante l'aumento delle minacce digitali e l'evoluzione delle tecnologie di automazione. Anche sul fronte ingegneristico navale il tema dell'evoluzione delle minacce *cyber* è stato affrontato in modo strutturato. L'International association of classification societies (Iacs) – organismo che stabilisce gli standard tecnici per progettare, costruire e manutenere le navi – ha introdotto due importanti aggiornamenti obbligatori dal prima luglio 2024: l'UR E26 che è dedicato alla *cyber-resilience* delle navi e che impone alle nuove costruzioni di adottare processi strutturati basati sul *framework* Nist. E l'UR E27 che si concentra invece sulla resilienza dei sistemi e delle attrezzature di bordo, richiedendo che ogni componente digitale sia progettato con requisiti minimi di sicurezza (ad esempio inventario *hardware*, *test*, *backup*, Sdlc - Ciclo di vita dello sviluppo del software sicuro) e una protezione rafforzata se connesso a reti esterne.
I regolamenti, comunque, da soli non bastano. I rischi informatici si moltiplicano anche per fattori strutturali e industriali. Uno dei principali riguarda i cosiddetti sistemi *legacy*, ovvero tecnologie operative (Ot) obsolete e ancora largamente diffuse a bordo delle navi e nei sistemi portuali. Questi dispositivi, spesso non aggiornabili o privi di livelli di protezione adeguati, rappresentano elementi di vulnerabilità facilmente sfruttabili da *cyber*-criminali. Inoltre, la crescente dipendenza dalla *supply chain* tecnologica cinese rappresenta una non trascurabile criticità. Nel 2024 i cantieri navali cinesi hanno realizzato circa il 90% della capacità portacontainer ordinata a livello globale. Questa concentrazione espone l'intero settore a possibili vulnerabilità di origine geopolitica e a intrusioni attraverso *backdoor* digitali o componenti compromessi. In conclusione, la crescente digitalizzazione del settore e l'integrazione dell'intelligenza artificiale agentica renderanno i sistemi infrastrutturali marittimi ancora più suscettibili a rischi informatici, e le decisioni autonome di sistemi intelligenti, senza supervisione umana, aumenteranno la possibilità di azioni malevoli o errori imprevisti che potrebbero compromettere la sicurezza operativa. La necessità di garantire sistemi di protezione robusti e una resilienza adeguata è ora più urgente che mai.