



Attacco Cyber ai freezer francesi e risposta NATO: la nuova frontiera del sabotaggio cibernetico ai danni dei civili

Pubblicato il 14/10/2026

Nella notte tra domenica e lunedì, **un'operazione informatica di inedita precisione ha preso il controllo dei sistemi di refrigerazione di oltre 350 supermercati in Francia**, appartenenti alle principali catene distributive (Carrefour, Monoprix, Intermarché, Coopérative U). **Alterando i parametri termici e portando le celle frigorifere fino a 50 gradi centigradi**, l'attacco ha trasformato le unità di congelamento in veri e propri forni, costringendo le aziende al macero immediato di tonnellate di alimentari.

L'attacco non ha presentato richieste di riscatto (escludendo il cybercrimine a scopo di estorsione) né rivendicazioni d'impatto ideologico. Ha sfruttato sistemi di controllo IoT dell'azienda danese Danfoss obsoleti o con firmware non aggiornato, dimostrando come vettori a bassa complessità tecnica possano generare enormi danni economici e psicologici sulla

popolazione.

Gli apparati d'intelligence di Parigi e l'agenzia nazionale ANSSI collegano **l'incursione alle operazioni ibride della Federazione Russa sul territorio europeo**, volte a destabilizzare la resilienza civile dei Paesi membri dell'Unione Europea e della NATO senza superare la soglia di un attacco armato esplicito.

L'Italia e la Nuova Governance ACN-Difesa

L'evento transalpino ha trovato immediato riscontro nell'audizione del Direttore Generale dell'ACN, Andrea Quacivi, davanti alle Commissioni Difesa e Affari Esteri del Senato. Pur rassicurando sull'assenza delle specifiche configurazioni vulnerabili nelle catene italiane, **Quacivi ha rimarcato l'urgenza di innalzare la postura di aggiornamento software nella PA e nelle aziende strategiche.**

Sotto la spinta del Disegno di Legge recante la firma del Ministro della Difesa Guido Crosetto (con la regia del Sottosegretario Alfredo Mantovano), l'Italia sta formalizzando il «*Piano di gestione delle crisi di cybersicurezza su vasta scala*». Il provvedimento stabilisce una duplice catena di comando basata sui concetti di "responsabilità primaria" e "supporto":

- **Fronte Civile (ACN):** Mantiene la funzione di coordinatore in capo per garantire la resilienza sistemica del Paese e la risposta agli incidenti critici.
- **Fronte Militare (Stato Maggiore della Difesa):** Riceve la responsabilità esplicita di garantire, anche in tempo di pace, la tutela dello spazio cibernetico di interesse nazionale, condotta tramite operazioni difensive e di risposta sia in Patria che all'estero.

Escalation della Minaccia Cyber sul Territorio Nazionale

I dati forniti dall'ACN per i primi nove mesi del 2026 tracciano un panorama di vera e propria escalation condotta da attori statali (Russia, Cina, Corea del Nord e Iran):

I Numeri della Minaccia Cyber in Italia (ACN 2026)

- **Eventi Cyber Rilevati:** 3.271 nei primi 9 mesi del 2026 (rispetto ai 2.729 dell'intero 2025).

- **Incidenti con Impatto Confermato:** 1.922 nel 2026, con un incremento del **+212%** rispetto ai 615 del 2025.
- **Notifiche Direttiva NIS 2:** Oltre 1.500 comunicazioni da Pubbliche Amministrazioni e imprese strategiche.
- **Allerta Preventiva:** Circa 72.000 alert e segnalazioni diramate dallo CSIRT Italia.

Il Dilemma NATO sull'Articolo 5 e la Deterrenza Ibrida

L'incursione nei supermercati francesi si inserisce in una serie di attacchi grigi verificatisi in Europa: affondamento di mercantili nel Mar Nero via droni, sabotaggi GPS e tentativi di paralisi dei server ospedalieri. Il Presidente del Comitato Militare Atlantico, ammiraglio Giuseppe Cavo Dragone, ha ribadito che la NATO dispone di capacità di risposta proporzionata e bilanciata, sia visibile sia coperta.

Nonostante le linee guida NATO approvate a partire dal 2016 prevedano formalmente l'attivazione dell'**Articolo 5** (clausola di difesa collettiva) anche di fronte ad attacchi ibridi o cibernetici, la reale "linea rossa" resta rigorosamente secretata per preservare l'effetto di deterrenza. Tuttavia, come sottolineato da analisti militari, la mancanza di una soglia pubblica e le incertezze geopolitiche sulla fermezza della risposta collettiva rischiano di incoraggiare avversari statali a proseguire le operazioni destabilizzanti a bassa intensità ma ad altissimo impatto economico e sociale.

Valutazione Conclusiva per la Difesa

La protezione dello spazio cibernetico non può più essere scissa dalla difesa della sovranità nazionale. È indispensabile accelerare l'implementazione delle reti ad alta resilienza, stringere il raccordo tra industria civile e strumento militare e rafforzare le capacità offensive e difensive dell'Alleanza nel dominio cyber.