

Fort Bragg: contractor accusato di fuga di notizie riservate e furto di materiale delle Special Forces

Pubblicato il 05/11/2026

Un ex contractor di Fort Bragg, il trentasettenne James Thomas Ashbacher di Spring Lake (North Carolina), è stato arrestato con l'accusa di aver violato gravemente i protocolli di sicurezza nazionale. L'indagine, condotta dal Dipartimento di Giustizia statunitense, ha portato a un'incriminazione formale per trasmissione illecita e detenzione di informazioni di difesa nazionale, oltre al furto di materiale militare sottratto a un'unità di Forze Speciali dell'Esercito, tra cui dispositivi di visione notturna rinvenuti durante una perquisizione domiciliare.

Il caso riaccende i riflettori su una criticità sistemica che attraversa i moderni apparati di difesa occidentali: il controllo e la tutela del segreto operativo all'interno delle catene di supporto logistico e tecnologico.

La Violazione: Tattiche Sensibili e Call Sign Esposti online

Secondo quanto emerso dall'impianto accusatorio, Ashbacher — che deteneva un'abilitazione di sicurezza di livello *top-secret* — avrebbe pubblicato online immagini e video classificati, esponendo involontariamente o deliberatamente dettagli cruciali relativi alle tattiche, alle procedure operative e ai *call sign* di reparti speciali dell'Esercito.

La diffusione di tali contenuti su piattaforme digitali rappresenta una minaccia diretta alla **sicurezza delle operazioni (OPSEC)**. La rivelazione di segnali di chiamata, schemi di movimento e metriche di ingaggio offre agli attori ostili elementi di analisi preziosi per il tracciato delle comunicazioni e l'identificazione preventiva dei dispositivi di comando e controllo (C2).

Il Fattore "Insider Threat" e l'Affidabilità della Componente Civile

L'episodio evidenzia una vulnerabilità strutturale legata all'impiego massiccio di personale civile e contractor privati all'interno di installazioni e comandi strategici.

- **La complessità tecnologica:** La transizione verso scenari di guerra multi-dominio e l'adozione di sistemi digitali avanzati (CJADC2) richiedono un supporto tecnico specialistico che le sole forze in servizio permanente non possono coprire interamente.
- **Il rischio di sottomissione dei controlli:** L'accesso esteso a banche dati classificate da parte di personale non militare riduce inevitabilmente l'efficacia dei filtri di lealtà istituzionale e di cultura della sicurezza, tradizionalmente radicati nei corpi combattenti.

La gestione di episodi simili impone una revisione drastica dei protocolli di *vetting* e dei sistemi di monitoraggio passivo (Data Loss Prevention) all'interno delle basi e dei comandi di proiezione.

Lezioni per la Difesa Europea e Nazionale

Il caso di Fort Bragg offre spunti di riflessione immediati anche per il contesto europeo e italiano, impegnato nella ridefinizione delle proprie riserve strategiche e dei comandi interforze:

1. **La protezione del perimetro informativo:** La sovranità tecnologica e la digitalizzazione dei teatri operativi non devono prescindere da una compartimentazione rigida dei dati sensibili.
2. **La salvaguardia del patrimonio operativo:** La compromissione di equipaggiamenti critici come i visori notturni dimostra che la vulnerabilità non è solo cibernetica, ma tocca la dimensione fisica della catena logistica.

Link notizia: https://www.military.com/fort-bragg-contractor-charged-with-leaking-classified-special-operations-secrets