

Fort Bragg: contractor accused of leaking classified information and stealing Special Forces equipment

Published on 05/11/2026

A former Fort Bragg contractor, 37-year-old James Thomas Ashbacher of Spring Lake (North Carolina), was arrested on charges of seriously violating national security protocols. The investigation, conducted by the U.S. Department of Justice, resulted in a formal indictment for the unlawful transmission and retention of national defense information, as well as the theft of military equipment taken from an Army Special Forces unit, including night-vision devices found during a search of his home.

The case once again highlights a systemic weakness affecting modern Western defense establishments: the control and protection of operational secrecy throughout logistical and technological support chains.

The Breach: Sensitive Tactics and Call Signs Exposed Online

According to the charges, Ashbacher — who held a *top-secret* security clearance — allegedly posted classified images and videos online, inadvertently or deliberately exposing critical details concerning tactics, operational procedures, and the *call signs* of Army special units.

The dissemination of such content on digital platforms poses a direct threat to **operations security (OPSEC)**. The disclosure of call signs, movement patterns, and engagement metrics provides hostile actors with valuable analytical data for communications tracking and the advance identification of command-and-control (C2) assets.

The Insider Threat Factor and the Reliability of the Civilian Component

The episode highlights a structural vulnerability associated with the extensive use of civilian personnel and private contractors within strategic installations and commands.

- **Technological complexity:** The transition toward multidomain warfare and the adoption of advanced digital systems (CJADC2) require specialized technical support that permanent active-duty forces alone cannot fully provide.
- **The risk of weakened safeguards:** Extensive access to classified databases by nonmilitary personnel inevitably reduces the effectiveness of institutional loyalty and security-culture filters, traditionally embedded in combat units.

Managing similar incidents requires a thorough review of *vetting* protocols and passive monitoring systems (Data Loss Prevention) within bases and power-projection commands.

Lessons for European and National Defense

The Fort Bragg case also offers immediate lessons for the European and Italian context, which is redefining its strategic reserves and joint commands:

1. **Protecting the information perimeter:** Technological sovereignty and the digitization of operational theaters must be accompanied by strict compartmentalization of sensitive data.
2. **Safeguarding operational assets:** The compromise of critical equipment such as night-vision devices shows that the vulnerability is not solely cyber-related, but also affects the physical dimension of the logistics chain.

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