Minaccia Jihadista interna al 66º Reggimento fanteria aeromobile "Trieste"

Pubblicato il 26/10/2026

Un'indagine coordinata dalla Procura della Repubblica di Napoli e condotta dalla DIGOS in sinergia con l'AISI ha riacceso i riflettori sui rischi di infiltrazione e radicalizzazione all'interno delle strutture di difesa istituzionali.
L'attività investigativa vede coinvolto un militare di vent'anni, originario di Napoli e in servizio a Forlì presso la caserma "De Gennaro", sede del **66° Reggimento Fanteria Aeromobile "Trieste"**.

Le evidenze investigative e la catena di prevenzione

L'inchiesta nasce da un'attivazione dell'**AISI** (Agenzia Informazioni e Sicurezza Interna), che ha monitorato tracce di propaganda d'ispirazione jihadista sul web. L'analisi e il tracciamento informatico condotto dagli specialisti hanno consentito di risalire all'identità digitale del giovane soldato.

Le ipotesi di reato formulate dagli inquirenti riguardano l'**apologia di terrorismo**, aggravate dall'impiego di strumenti informatici e telematici. Secondo quanto ricostruito:

- **Attività di rete:** Il militare avrebbe condiviso materiali multimediali d'esaltazione di organizzazioni terroristiche quali *al-Qa'ida* e lo *Stato Islamico* (Daesh), celebrando figure apicali del jihadismo globale.
- **Perquisizioni locali e personali:** La DIGOS di Napoli ha eseguito decreti di perquisizione sequestrando dispositivi informatici (smartphone, PC, supporti di memoria) destinati agli accertamenti forensi.
- **I riscontri in caserma:** Durante i controlli eseguiti presso le strutture del 66° Reggimento a Forlì, gli investigatori hanno rinvenuto e sequestrato una bandiera nera riconducibile all'ISIS, custodita in un cassetto ed ex ante utilizzata dal giovane per autosfide grafiche e fotografie.

Lo Stato Maggiore della Difesa e i comandi di vertice sono stati tempestivamente informati per l'adozione delle correlate contromisure disciplinari e di sicurezza della sede.
Come sottolineato dalle fonti investigative, il procedimento si trova nella fase delle indagini preliminari. I dispositivi e il materiale sequestrato saranno sottoposti ad analisi tecnica; la responsabilità penale dell'indagato dovrà essere accertata nelle sedi giudiziarie competenti nel rispetto della presunzione di innocenza.

Cos'è l'Insider Threat: la prospettiva della Counter-Intelligence

Il caso del 66° Reggimento riconduce sul piano dottrinale al concetto politico-militare di **Insider Threat** (minaccia interna).
In ambito intelligence e *Force Protection*, un *insider threat* si definisce come un individuo che sfrutta il proprio accesso autorizzato — fisico o logico — a strutture, reti informatiche, armamenti o informazioni riservate di un'organizzazione per arrecare danno alla sicurezza nazionale, compiere atti di sabotaggio, spionaggio o agevolare entità ostili e terroristiche.
I vettori di vulnerabilità dell'insider si articolano solitamente su tre direttrici principali:

1. **Ideologica e di Radicalizzazione:** L'adesione consapevole o progressiva a narrative estremiste (Jihadismo, suprematismo, sovversione).

2. **Coercitiva o Economica:** Il condizionamento da parte di servizi informativi esteri o attori non statali tramite ricatto, vulnerabilità finanziarie o dipendenze.
3. **Informatica (*Cyber Insider*):** L'impiego delle proprie credenziali per sottrarre od ostacolare il patrimonio informativo della Difesa.

Il fenomeno nei teatri operativi: la lezione dell'Afghanistan (*Green-on-Blue Attacks*)

Se nel contesto di guarnigione nazionale l'insider threat si manifesta prevalentemente in forme di radicalizzazione silente e propaganda, nei teatri d'operazione ad alta intensità ha rappresentato una delle sfide tattiche e strategiche più complesse.
L'esempio più sistematico e drammatico si è registrato durante la campagna della missione ISAF/Resolute Support in **Afghanistan**.
Nel gergo NATO, i codici cromatici identificano le forze in campo:

- **Blue:** Le forze della coalizione internazionale (NATO e alleati).
- **Green:** Le forze di sicurezza locali (Afghan National Army - ANA, e Afghan National Police - ANP).

Gli **attacchi Green-on-Blue** (o *Insider Attacks*) si verificavano quando elementi delle forze armate o di polizia afghane — oppure insorti talebani infiltrati indossando l'uniforme governativa — volgevano le armi contro gli istruttori e i soldati della coalizione NATO durante attività di addestramento (*Partnering/Mentoring*), pattugliamenti congiunti o all'interno delle basi operative (*FOB - Forward Operating Bases*).

Le cause scatenanti nei teatri Asimmetrici

L'analisi di CI (*Counter-Intelligence*) condotta dalle forze alleate in Afghanistan evidenziò come gli attacchi *Green-on-Blue* scaturissero da tre fattori chiave:

- **Infiltrazione Pianificata:** Attori ostili (Talebani, Rete Haqqani) reclutavano soggetti da inserire nelle accademie o nei centri di reclutamento afghani al solo fine di compiere attentati.

- **Radicalizzazione *In-Service*:** Soldati regolarmente arruolati che si radicalizzavano progressivamente a causa della propaganda d'influenza o delle perdite subite tra i propri familiari.
- **Incomprensioni Culturali e *Grievances*:** Tensioni personali, attriti quotidiani o percezione di offesa ai valori religiosi/culturali, cavalcati dalla sovversione ideologica.

Rilevanza per la sicurezza delle Forze Armate

L'episodio registrato a Forlì evidenzia come **le dinamiche di radicalizzazione e la minaccia asimmetrica non siano confinate ai teatri operativi esteri,** ma richiedano un monitoraggio costante dei processi di reclutamento e della condotta del personale in servizio. Il coordinamento integrato tra l'intelligence di sicurezza (AISI), le articolazioni investigative delle Forze di Polizia (DIGOS, Servizio per il Contrasto all'Estremismo e al Terrorismo Esterno) e le strutture di sicurezza militare dello Stato Maggiore della Difesa costituisce il baluardo fondamentale per individuare tempestivamente i segnali premonitori (*left of launch*) e preservare l'integrità e la sicurezza delle istituzioni repubblicane.

Link notizia: https://www.facebook.com/share/p/1Dx9PD4Pmm/