USA, l’eccesso di informazioni pubbliche del personale della Difesa rende la cybersicurezza sempre più difficile

Pubblicato il 24/11/2025

Il Pentagono si trova sempre più esposto a rischi informatici a causa della quantità crescente di **informazioni pubbliche** diffuse online da piattaforme civili, dispositivi personali, comunicazioni ufficiali e attività social. A lanciare l’allarme è un rapporto pubblicato il 17 novembre dalla **Government Accountability Office (GAO)**, che evidenzia come questa mole di dati tracciabili stia compromettendo la capacità del Dipartimento della Difesa (DoD) di proteggere operazioni, infrastrutture e personale.

Il problema: troppe tracce digitali accessibili a chiunque

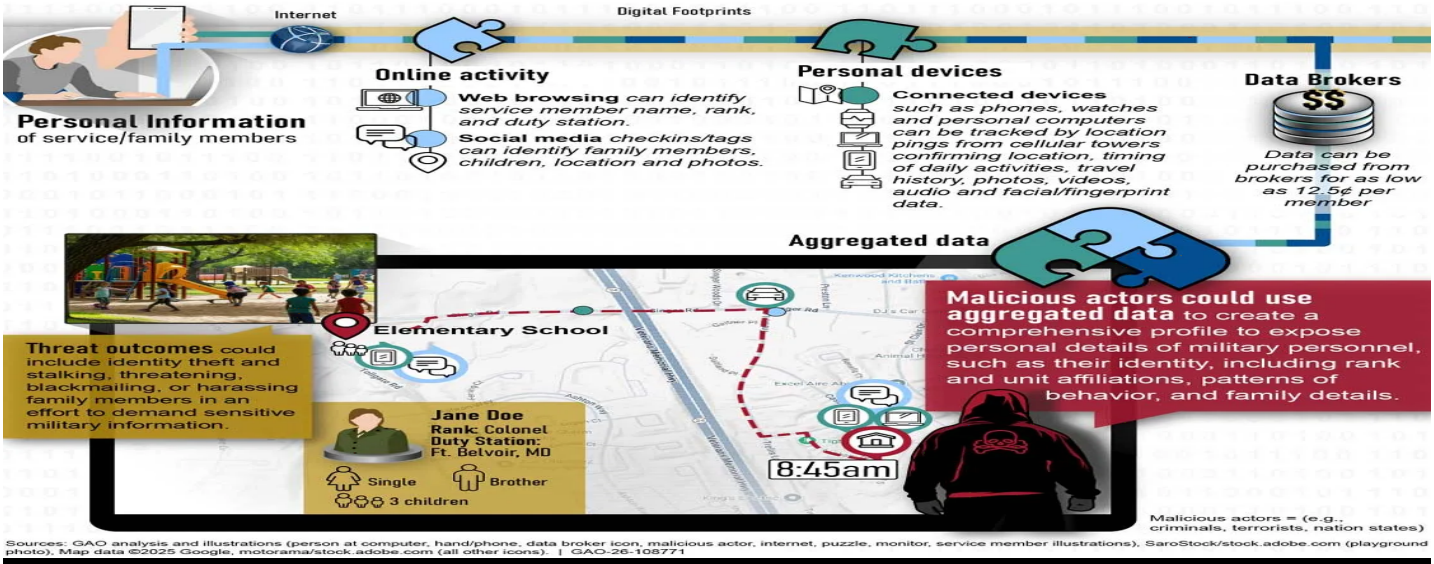
Secondo la GAO, la cosiddetta “rivoluzione digitale” ha prodotto un’enorme quantità di informazioni che possono essere raccolte, combinate e sfruttate da attori ostili. Movimenti di

navi e velivoli, foto geolocalizzate, comunicazioni online e perfino tracce lasciate da dispositivi personali finiscono spesso in chiaro sul web.

Questi dati permettono a gruppi criminali, intelligence avversarie e hacker di:

- **ricostruire rotte o schemi operativi;**
- **individuare con facilità personale militare e ruoli sensibili;**
- **anticipare la presenza di asset strategici;**
- **mettere a rischio la sicurezza delle missioni.**

La GAO sottolinea che informazioni apparentemente innocue — coordinate marittime, comunicati stampa, attività social — possono essere aggregate per prevedere, ad esempio, la rotta di una portaerei o lo spostamento di una task force.



Scenario di possibili minacce derivanti dall’esposizione delle informazioni sul personale del Dipartimento della Difesa degli Stati Uniti - Copyright U.S. Government Accountability Office

Pentagono in ritardo: formazione insufficiente e valutazioni mancanti

Il rapporto analizza dieci componenti del Dipartimento della Difesa, tra cui **NSA, DIA, Cyber Command, SOCOM e tutte le Forze Armate USA**. Il risultato è chiaro: quasi tutti hanno lacune significative nella gestione dei rischi legati alle informazioni pubbliche.

La GAO rileva che:

- **solo lo U.S. Special Operations Command (SOCOM)** ha implementato una formazione completa su questi rischi;
- **8 componenti su 10** non hanno svolto le valutazioni obbligatorie nelle aree di force protection, insider threat, mission assurance e OPSEC;
- molte direttive interne sono **incomplete**, troppo specifiche o applicate in modo non uniforme.

In altre parole, il Pentagono non dispone di un quadro solido e omogeneo per fronteggiare un rischio che sta crescendo esponenzialmente.

Scenario delle possibili minacce derivanti dalla divulgazione delle operazioni navali - Copyright U.S. Government Accountability Office

Regole frammentate e minacce crescenti

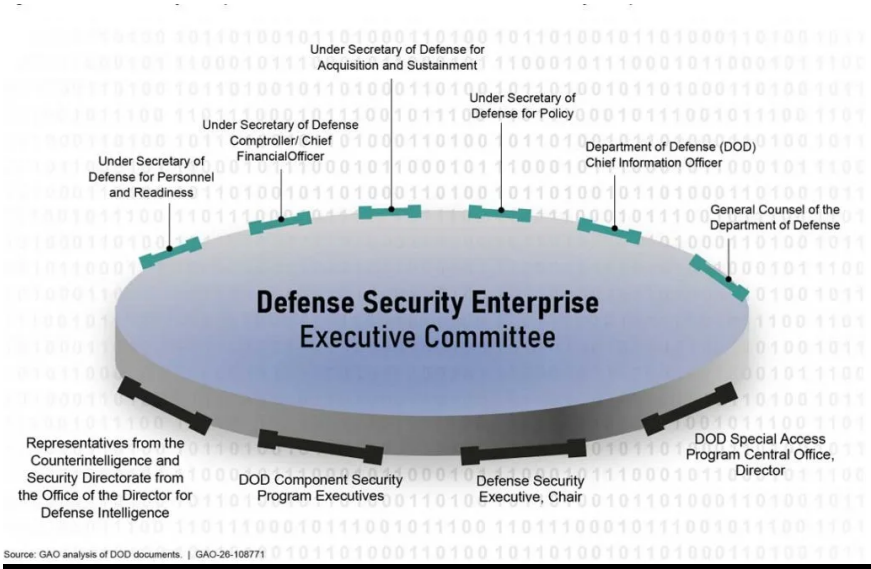
Tre dei cinque uffici collegati al Segretario alla Difesa hanno emesso politiche per limitare l'esposizione digitale del personale, ma secondo la GAO queste linee guida sono "troppo ristrette" e non coprono tutti gli aspetti della sicurezza.

La complessità del problema richiede un approccio centralizzato. Per questo il rapporto indica il **Defense Security Enterprise Executive Committee** come l'organo più adatto per coordinare un'analisi dipartimentale e uniformare le politiche sul digital footprint.

Senza una strategia unificata, avverte la GAO, il Dipartimento della Difesa rischia di:

- **non riuscire a valutare correttamente le minacce**;

- **non proteggere la privacy del personale;**
- **compromettere missioni sensibili**;
- **esporre il Paese a vulnerabilità di sicurezza nazionale.**



Organigramma del Comitato Esecutivo della Defense Security Enterprise con i principali funzionari del Dipartimento della Difesa - Copyright U.S. Government Accountability Office

Dodici raccomandazioni per un Pentagono (e non solo) più protetto

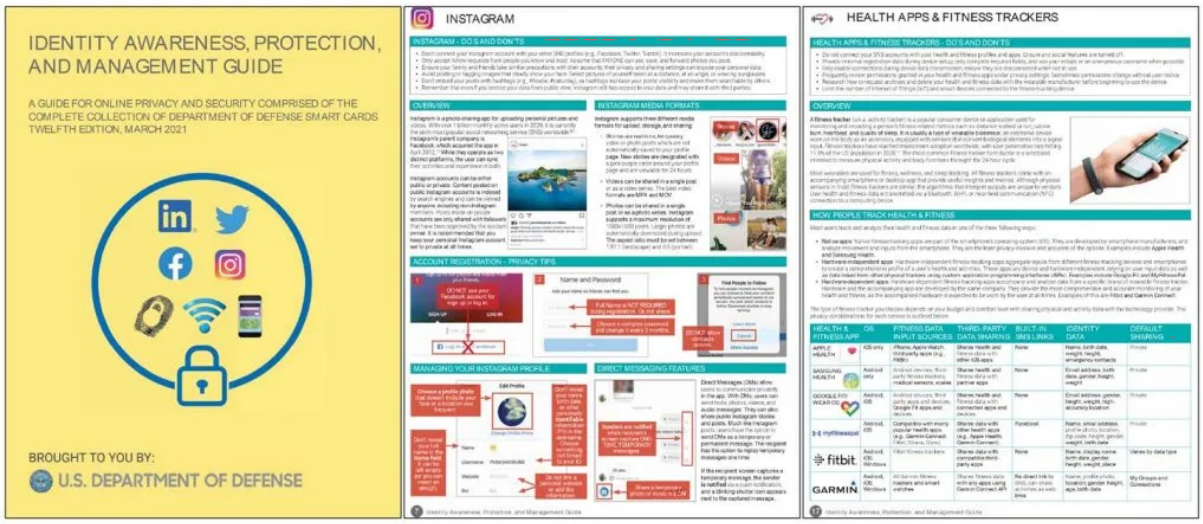
Per affrontare il problema, la GAO ha formulato **12 raccomandazioni**, tra cui:

- **rafforzare la formazione su rischi e comportamenti digitali;**
- **completare le valutazioni di sicurezza mancanti;**
- **coordinare le politiche tra tutte le componenti del DoD;**
- **limitare e monitorare la diffusione di informazioni digitali accessibili al pubblico;**
- **verificare come dati apparentemente innocui possano essere aggregati da attori ostili.**

Il Dipartimento della Difesa ha accettato **11 raccomandazioni su 12**, concordando solo parzialmente con una.

Il rapporto chiede inoltre al Segretario alla Difesa **Pete Hegseth** di vigilare personalmente sull’implementazione delle misure mancanti, soprattutto in ambiti strategici come force protection e insider threat.

Il problema non riguarda solo il Pentagono. Negli ultimi anni, sia **Camera** che **Senato** hanno presentato disegni di legge per limitare l'esposizione digitale del personale della Difesa, consapevoli che l'impronta digitale è ormai diventata un potenziale bersaglio per potenze straniere, cybercriminali e gruppi terroristici.



Source: DOD Identity Awareness, Protection, and Management Guide. | GAO-26-108771

Guide dedicate alla sicurezza online dei militari USA, con istruzioni per usare in modo sicuro social network e app - Copyright U.S. Government Accountability Office

Conclusione: un monito anche per l'Italia

Il messaggio della GAO è netto: la cybersicurezza americana è sempre più difficile da garantire a causa dell'enorme quantità di dati pubblici che riguardano operazioni, asset e personale militare.
La sfida non è solo tecnologica, ma anche culturale. Ridurre il digital footprint, formare adeguatamente il personale e uniformare le procedure sono passaggi indispensabili per proteggere il Pentagono in un mondo in cui ogni traccia digitale può diventare un'arma nelle mani sbagliate.

Per **Europa e Italia**, questo rapporto dovrebbe essere letto come un campanello d'allarme. Anche le Forze Armate europee, incluse le Forze Armate italiane, sono sempre più esposte alla stessa combinazione di fattori: uso massivo di dispositivi personali, social network, piattaforme civili di tracking e comunicazione istantanea.

Se gli Stati Uniti, con mezzi e strutture imponenti, faticano a gestire l'impatto delle "informazioni pubbliche" sulla sicurezza, è evidente che per i Paesi europei la priorità deve

essere:

- **integrare stabilmente il rischio del digital footprint nelle dottrine di sicurezza e difesa;**
- **rafforzare formazione e sensibilizzazione di militari, civili della Difesa e contractor;**
- **sviluppare politiche comuni NATO/UE sulla gestione delle tracce digitali operative.**

Per l’Italia, sempre più inserita in contesti multinazionali, anticipare questi rischi significa **proteggere meglio i propri uomini e donne in uniforme**, preservare la segretezza operativa e collocarsi tra quei Paesi che non subiscono la rivoluzione digitale, ma la governano anche sul piano della sicurezza.

gao-26-108771Download

Link notizia: https://www.gao.gov/products/gao-26-108771