



L'APP Strava espone i militari USA: le corse pubblicate online potrebbero aver aiutato l'Iran a individuare gli obiettivi

Pubblicato il 17/08/2026

Una corsa di pochi chilometri, registrata con uno smartwatch e pubblicata online, può sembrare un'informazione insignificante. Ma quando centinaia di militari ripetono la stessa operazione giorno dopo giorno, quelle tracce GPS possono trasformarsi in una vera fonte d'intelligence.

È quanto emerge da un'inchiesta del team **Data and Forensics di Sky News**, che ha individuato **oltre 1.300 utenti di Strava impegnati a condividere allenamenti provenienti da installazioni militari statunitensi in Medio Oriente**. Migliaia di attività hanno reso visibili percorsi, orari e abitudini del personale, permettendo di osservare non soltanto la vita quotidiana all'interno delle basi, ma anche variazioni nella presenza delle truppe, trasferimenti e spostamenti verso altre installazioni. In alcuni casi si tratta persino di basi non indicate sulle normali mappe pubbliche.

Il problema è aggravato dal fatto che molti degli utenti individuati da Sky News utilizzavano **nome e cognome reali**, associando quindi una posizione geografica e una routine quotidiana a persone identificabili. Per un servizio d'intelligence ostile non si tratta più soltanto di sapere dove si trovi una struttura militare, ma potenzialmente di capire **chi vi lavora, dove si sposta e come cambiano le sue abitudini**.

Dal fitness all'intelligence: il “pattern of life”

Una singola traccia GPS ha un valore limitato. Centinaia o migliaia di tracce raccolte nel tempo raccontano invece qualcosa di molto più importante.

Gli analisti parlano di **“pattern of life”**, cioè della ricostruzione delle abitudini e dei ritmi ricorrenti di una persona o di un'organizzazione: dove si concentra il personale, quali edifici vengono frequentati, in quali orari avvengono determinati movimenti e, soprattutto, quando queste abitudini cambiano.

È proprio questo uno degli aspetti più inquietanti emersi dall'indagine.

Sky News ha analizzato le attività provenienti dalla **Muwaffaq Al Salti Air Base, in Giordania**. Prima dell'inizio della guerra, il 28 febbraio 2026, il personale statunitense pubblicava centinaia di corse distribuite in diverse aree dell'installazione.

Quando le attività sono ricomparse in aprile, durante il cessate il fuoco, qualcosa era cambiato: **il 76% delle corse iniziava o terminava nello stesso punto**, identificato da Sky News con le caserme situate nell'angolo orientale della base.

Il **17 luglio l'Iran ha attaccato proprio quelle caserme**, provocando la morte di tre militari.

Questo non dimostra che siano state le tracce di Strava a determinare la scelta dell'obiettivo, ma mostra quanto informazioni apparentemente innocue possano contribuire a confermare la presenza e la concentrazione del personale in una determinata area.

Il caso del contractor della Marina USA in Bahrein

Ancora più significativo è quanto ricostruito a **Manama, in Bahrein**.

Il 1° marzo l'Iran ha lanciato attacchi di rappresaglia contro diverse installazioni statunitensi in Medio Oriente, compresa una grande base navale nella capitale del Bahrein. Prima degli

attacchi, una parte consistente del personale era stata evacuata dalla struttura e trasferita in edifici residenziali e alberghi della città.

Sky News ha individuato l'account Strava di un contractor della US Navy che, fino alla settimana precedente all'inizio della guerra, registrava abitualmente le proprie corse intorno alla base.

Poi le attività si interrompono.

Dopo due giorni il profilo torna attivo, ma in un luogo diverso: il contractor comincia a registrare giri di corsa **nel cortile del Crowne Plaza di Manama**.

Se qualcuno avesse seguito quel profilo, avrebbe potuto dedurre che almeno parte del personale collegato alla base era stata trasferita nell'albergo.

Sei giorni più tardi l'Iran colpì anche il Crowne Plaza durante gli attacchi contro l'area della base navale. Secondo quanto riportato da Sky News, due dipendenti del Pentagono rimasero feriti.

Anche in questo caso non esistono prove pubbliche che dimostrino che Teheran abbia selezionato l'hotel grazie a Strava.

Joseph Jarnecki, ricercatore del **Royal United Services Institute (RUSI)** ed esperto di sicurezza nazionale, ha tuttavia definito «**completamente plausibile**» che l'Iran abbia utilizzato anche informazioni provenienti da Strava, insieme ad altre fonti, per seguire il trasferimento del personale statunitense.

L'Iran osserva Strava?

Secondo Jonathan Hackett, esperto di operazioni speciali e autore di *Iran's Shadow Weapons*, Teheran starebbe «**quasi certamente**» **utilizzando applicazioni come Strava per monitorare gli spostamenti delle forze statunitensi in Medio Oriente**.

Hackett attribuisce la continua esposizione di informazioni di questo tipo a una combinazione di scarsa applicazione delle regole e insufficiente consapevolezza del rischio da parte del personale.

È importante però distinguere i due livelli.

Che Strava costituisca una possibile fonte OSINT utile a un avversario è ampiamente riconosciuto. Che l'Iran abbia effettivamente utilizzato una determinata corsa per programmare uno specifico bombardamento **non è invece stato dimostrato pubblicamente**.

L'inchiesta evidenzia soprattutto una serie di correlazioni molto significative tra dati pubblicamente disponibili, spostamenti del personale e obiettivi successivamente attaccati.

Il Pentagono aveva lanciato l'allarme già nel 2018

Il rischio non è nuovo.

Già nell'agosto **2018 il Dipartimento della Difesa statunitense aveva vietato al personale nelle aree operative l'utilizzo non autorizzato delle funzioni di geolocalizzazione** presenti su dispositivi, applicazioni e servizi.

Il provvedimento comprendeva esplicitamente fitness tracker, smartphone e applicazioni capaci di registrare la posizione dell'utente. Secondo il Pentagono, questi sistemi potevano rivelare **informazioni personali, ubicazioni, routine e persino il numero di militari presenti**, creando rischi per le operazioni.

La questione era esplosa proprio grazie alla diffusione delle mappe aggregate delle attività sportive: percorsi illuminati nel mezzo di zone desertiche apparentemente vuote potevano indirettamente rivelare la presenza di installazioni militari.

Otto anni dopo, il problema sembra tutt'altro che risolto.

12.000 allenamenti dalla base britannica di Akrotiri

Il fenomeno non riguarda soltanto gli Stati Uniti.

Sky News ha individuato militari britannici che continuavano a pubblicare attività dall'importante **base RAF di Akrotiri, a Cipro**, anch'essa divenuta obiettivo degli attacchi iraniani.

Dall'inizio del 2026 sarebbero stati individuati **circa 12.000 allenamenti pubblicati dall'interno della base**. Alcuni profili hanno inoltre consentito agli investigatori di seguire gli stessi utenti durante successivi dispiegamenti in altre località del Medio Oriente, comprese installazioni non indicate sulle mappe pubbliche.

L'indagine ha individuato persino **tre utenti Strava che registravano corse all'interno del centro di ricerca nucleare israeliano di Dimona**, una delle strutture più sensibili di Israele e già bersaglio di attacchi iraniani.

Lo smartphone come sensore d'intelligence involontario

Il caso Strava mostra un cambiamento fondamentale dell'intelligence moderna.

Non è necessario penetrare una rete militare classificata per ottenere informazioni operative utili. Smartphone, smartwatch, social network e applicazioni commerciali possono produrre continuamente piccoli frammenti di informazione.

Presi singolarmente significano poco.

Aggregati e analizzati nel tempo possono invece mostrare:

- la presenza o l'assenza di personale;
- l'aumento o la diminuzione dell'attività in una base;
- il trasferimento di militari verso altre strutture;
- gli edifici maggiormente frequentati;
- le routine quotidiane;
- l'identità di alcuni membri del personale;
- improvvise modifiche nelle abitudini che possono indicare una variazione dell'assetto operativo.

È esattamente il principio alla base dell'**OSINT**, l'intelligence ricavata da fonti aperte.

In questo scenario, il militare che pubblica la propria corsa non sta semplicemente raccontando quanti chilometri ha percorso: può inconsapevolmente trasformarsi in **un sensore che alimenta la raccolta informativa dell'avversario**.

Strava, da parte sua, ha dichiarato a Sky News di prendere molto seriamente sicurezza e privacy degli utenti e di mettere a disposizione numerosi controlli per limitare la visibilità dei contenuti, sottolineando che chi opera in professioni sensibili dovrebbe utilizzare queste

impostazioni in maniera appropriata.

Il problema, dunque, non è necessariamente l'applicazione.

È l'informazione che centinaia di persone continuano volontariamente a pubblicare.

E nell'era dell'OSINT, migliaia di corse apparentemente insignificanti possono finire per comporre una mappa molto più interessante per un servizio d'intelligence di quanto gli stessi utenti possano immaginare.

Fonti

- **Sky News - Data and Forensics, 12 agosto 2026: “Strava users sharing sensitive data from US bases targeted by Iran”**
- **U.S. Department of Defense, 6 agosto 2018: “New Policy Prohibits GPS Tracking in Deployed Settings”**