



The Strava App Exposes US Military: Runs Published Online Could Have Helped Iran Identify Targets

Published on 17/08/2026

A few kilometers run, recorded with a smartwatch and published online, may seem like insignificant information. But when hundreds of military personnel repeat the same operation day after day, those GPS traces can transform into a real source of intelligence.

This is what emerges from an investigation by the **Sky News Data and Forensics team**, which identified **over 1,300 Strava users sharing workouts from US military installations in the Middle East**. Thousands of activities made visible routes, times, and habits of personnel, allowing observation not only of daily life within the bases but also variations in troop presence, transfers, and movements to other installations. In some cases, these are even bases not indicated on standard public maps.

The problem is compounded by the fact that many of the users identified by Sky News used **their real names and surnames**, thus associating a geographic position and daily routine

with identifiable people. For a hostile intelligence service, it is no longer merely about knowing where a military facility is located, but potentially understanding **who works there, where they move, and how their habits change.**

From Fitness to Intelligence: the "Pattern of Life"

A single GPS trace has limited value. Hundreds or thousands of traces collected over time tell something much more important.

Analysts speak of "**pattern of life**", that is, the reconstruction of the habits and recurring rhythms of a person or organization: where personnel concentrate, which buildings are frequented, what times certain movements occur, and most importantly, when these habits change.

This is precisely one of the most disturbing aspects that emerged from the investigation.

Sky News analyzed activities from the **Muwaffaq Al Salti Air Base in Jordan**. Before the war began on February 28, 2026, US personnel published hundreds of runs distributed across various areas of the installation.

When activities reappeared in April, during the ceasefire, something had changed: **76% of the runs started or ended at the same point**, identified by Sky News as the barracks located in the eastern corner of the base.

On **July 17, Iran attacked those barracks**, killing three military personnel.

This does not prove that Strava traces determined the choice of target, but it shows how apparently innocent information can contribute to confirming the presence and concentration of personnel in a specific area.

The Case of a US Navy Contractor in Bahrain

Even more significant is what was uncovered in **Manama, Bahrain**.

On March 1, Iran launched retaliatory attacks against several US installations in the Middle East, including a major naval base in Bahrain's capital. Before the attacks, a substantial part of the personnel had been evacuated from the facility and transferred to residential buildings and hotels in the city.

Sky News identified the Strava account of a US Navy contractor who, until the week before the war began, regularly recorded his runs around the base.

Then the activities stop.

After two days the profile becomes active again, but in a different location: the contractor begins recording runs **in the courtyard of the Crowne Plaza in Manama**.

If someone had been following that profile, they could have deduced that at least part of the personnel connected to the base had been transferred to the hotel.

Six days later, Iran also struck the Crowne Plaza during attacks on the naval base area. According to Sky News, two Pentagon employees were injured.

In this case too, there is no public evidence proving that Tehran selected the hotel thanks to Strava.

However, Joseph Jarnecki, a researcher at the **Royal United Services Institute (RUSI)** and national security expert, defined it as "**completely plausible**" that Iran used information from Strava, along with other sources, to track the transfer of US personnel.

Is Iran Watching Strava?

According to Jonathan Hackett, a special operations expert and author of *Iran's Shadow Weapons*, Tehran is "**almost certainly**" using applications like Strava to monitor the **movements of US forces in the Middle East**.

Hackett attributes the continued exposure of this type of information to a combination of poor rule enforcement and insufficient risk awareness among personnel.

However, it is important to distinguish between the two levels.

That Strava constitutes a possible OSINT source useful to an adversary is widely recognized. That Iran actually used a particular run to plan a specific bombing **has not been publicly demonstrated**.

The investigation highlights above all a series of very significant correlations between publicly available data, personnel movements, and subsequently attacked targets.

The Pentagon Had Sounded the Alarm Back in 2018

The risk is not new.

Already in August **2018**, the **US Department of Defense prohibited personnel in operational areas from unauthorized use of geolocation functions** present on devices, applications, and services.

The measure explicitly included fitness trackers, smartphones, and applications capable of recording the user's position. According to the Pentagon, these systems could reveal **personal information, locations, routines, and even the number of military personnel present**, creating operational risks.

The issue had exploded precisely due to the spread of aggregate maps of sports activities: routes illuminated in the middle of apparently empty desert zones could indirectly reveal the presence of military installations.

Eight years later, the problem seems far from solved.

12,000 Workouts from the British Akrotiri Base

The phenomenon does not only affect the United States.

Sky News identified British military personnel who continued to publish activities from the important **RAF Akrotiri base in Cyprus**, which also became a target of Iranian attacks.

Since the beginning of 2026, approximately **12,000 workouts posted from inside the base** would have been identified. Some profiles also allowed investigators to track the same users during subsequent deployments to other locations in the Middle East, including installations not indicated on public maps.

The investigation even identified **three Strava users recording runs inside the Israeli nuclear research center at Dimona**, one of Israel's most sensitive facilities and already a target of Iranian attacks.

The Smartphone as an Involuntary Intelligence Sensor

The Strava case shows a fundamental shift in modern intelligence.

It is not necessary to penetrate a classified military network to obtain useful operational information. Smartphones, smartwatches, social networks, and commercial applications can continuously produce small fragments of information.

Taken individually they mean little.

Aggregated and analyzed over time, however, they can show:

- the presence or absence of personnel;
- the increase or decrease in activity at a base;
- the transfer of military personnel to other facilities;
- the buildings most frequently visited;
- daily routines;
- the identity of some personnel members;
- sudden changes in habits that may indicate a shift in operational posture.

It is exactly the principle behind **OSINT**, intelligence derived from open sources.

In this scenario, the military personnel publishing their run is not simply reporting how many kilometers they covered: they can unknowingly become **a sensor feeding the adversary's information gathering**.

For its part, Strava told Sky News that it takes user security and privacy very seriously and provides numerous controls to limit content visibility, emphasizing that those in sensitive professions should use these settings appropriately.

The problem, therefore, is not necessarily the application.

It is **the information that hundreds of people continue willingly to publish**.

And in the age of OSINT, thousands of apparently insignificant runs can end up composing a much more interesting map for an intelligence service than the users themselves could imagine.

Sources

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